

从面试的角度来梳理.NET程序员的技术功底
以项目开发经理的眼光来审视编程知识的掌握

网络服务



附赠光盘，
含所有实例源代码
附赠光盘，含所有
实例源代码。

搭建、配置与管理大全 (Windows版)

赵松涛 编著

赵松涛

- ◎ 分六大部分，涵盖常见的.NET面试题
- ◎ 近百段示例代码，百余张插图，详细解析底层机制和原理
- ◎ 先问题分析，后参考答案，读者知其然更知其所以然
- ◎ 代码注释详尽，帮助读者快速理解代码
- ◎ 大量技巧和注意点，帮助读者快速提高技术水平



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

网络服务搭建、配置与管理大全 ——Windows版

刘晓辉 编著

书名:	责编:
社名:	校次:
开本:	正文页码:
文前页码:	排版员:
日期:	排版公司:
主管签字:	

电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书以 Windows Server 2008 为基础, 兼顾 Windows Server 2003, 全面深入地介绍了如何搭建、配置与管理各种 Windows 基础服务和应用服务, 包括活动目录服务、DHCP 服务、DNS 服务、WINS 服务、打印服务、Web 服务、FTP 服务、文件服务、WSS 服务、认证服务、终端服务、Windows 部署服务、WSUS 服务、NAP 服务、MOM 服务、ISA 服务, 以及网络防病毒服务等, 是 Windows 网络应用的完全技术手册。

本书突出实用性和可操作性, 理论讲解深入浅出, 通俗易懂。并且注重培养动手能力和分析能力。读者只需熟悉 Windows 基本操作, 按照书中讲解的知识即可轻松动手搭建所需的网络服务, 并且根据实际需要完成必要的配置和管理。

本书适用于正在从事网络管理工作的网络管理员、系统管理员、安全管理员、准备从事网络、系统和安全管理工作的本专科学生, 以及计算机网络爱好者。此外, 本书也可作为大专院校计算机网络专业的相关教材, 或课外参考资料。

未经许可, 不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有, 侵权必究。

图书在版编目(CIP)数据

网络服务搭建、配置与管理大全: Windows 版 / 刘晓辉编著. —北京: 电子工业出版社, 2009.3
(网管宝典)
ISBN 978-7-121-07880-4

I. 网… II. 刘… III. 服务器—操作系统(软件), Windows Server 2008 IV. TP316.86

中国版本图书馆 CIP 数据核字(2008)第 183562 号

责任编辑: 孙学瑛

印 刷: 北京京科印刷有限公司

装 订: 三河市鑫金马印装有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本: 850×1168 1/16 印张: 51.5 字数: 1560 千字

印 次: 2009 年 3 月第 1 次印刷

印 数: 3500 册 定价: 99.00 元(含光盘 1 张)

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 zltts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线: (010) 88258888。



前言

搭建网络的终极目的就是共享网络服务，因此网络管理员的重要职责之一，就是构建安全、稳定且功能丰富的网络基础服务和网络应用服务。尽管 Linux/UNIX 操作系统具有较高的系统稳定性和安全性，然而由于 Windows 网络操作系统具有无与伦比的易用性，而且其系统稳定性和安全性也有大幅的提高，因此大量中小型网络管理员都很自然地采用 Windows 作为服务器系统的平台。统计表明，Windows Server 系统占据服务器操作系统 70% 以上的市场份额。作为最新版本的 Windows Server 2008 操作系统，其运行效率更高，系统安全性更强，服务功能更丰富，更能发挥多核和 64 位架构的潜能；并且对硬件配置的要求与 Windows Server 2003 非常接近，能够更好地适应网络环境的变化和网络用户的需求。

本书内容



本书以 Windows Server 2008 服务器操作系统为基础、最新版本的应用服务程序为主导，深入介绍各种 Windows 基础服务和应用服务，包括安装 Windows Server 2003/2008 操作系统和 Server Core。

- 用于网络用户和资源管理的 Active Directory 服务。
- 用于 IP 地址管理的 DHCP 服务、用于域名管理的 DNS 服务、用于局域网中名称解析的 WINS 服务。
- 用于管理打印机的打印服务。
- 用于搭建 Web 网站的 WWW 服务。
- 用于文件下载和上传的 FTP 服务。
- 用于安全通信和身份认证的证书服务。
- 用于网络文件存储的文件服务和分布式文件系统。
- 用于信息资源共享的 Windows SharePoint Services 3.0 服务。
- 用于远程安装 Windows XP 及 Windows Server 2003 的 RIS 服务。
- 用于远程安装 Windows Vista 和 Windows Server 2008 的 Windows 部署服务。
- 用于系统补丁更新和管理的 WSUS 服务、用于远程管理服务器的终端服务。
- 用于对客户端接入进行安全限制的 NAP 服务、用于局域网服务器管理的 MOM 服务。
- 用于实现 Internet 连接共享和网络防火墙的 ISA 服务。
- 用于构建病毒防火墙的 Symantec 病毒服务。

本书特点



本书具有以下特点。

(1) 全面介绍了 Windows Server 2008 服务器搭建、配置与管理,借助差异化比较方式,分别讲述 Windows Server 2003 和 Windows Server 2008 版本在功能实现和操作上的异同,以及如何实现不同版本的升级、迁移和共存。

(2) 全面介绍 Microsoft 其他重要网络服务(如 Exchange、ISA、LCS、SMS、SPS 及 MOM 等)的最新版本,读者可以用其搭建并管理完整的网络服务体系,实现深入网络应用。一书在手,别无他忧!

(3) 突出实用性、针对性和技术性,紧贴 Windows 服务器的搭建实践。大量的经验、技巧和提示帮助读者避开各种危险的陷阱,迅速提高自己的技术水平。

本书由刘晓辉编著,李海宁、刘淑梅、赵卫东、杨伏龙、李文俊、王同明、石长征、郭腾、白华、陈志成、田俊乐、李寅、刘国增、王延杰、刘红、王淑江及王春海等也参与了部分章节的编写工作。笔者长期从事网络教学、实验和管理工作,规划、设计、论证、实施并验收过多个大中型网络建设项目,具有较高的理论水平和丰富的实践经验。曾经出版过 30 余部计算机类图书,均以易读、易学且实用的特点受到众多读者的一致好评。本书是笔者的又一呕心沥血之作,希望能对读者的网络搭建及管理工作有所帮助。

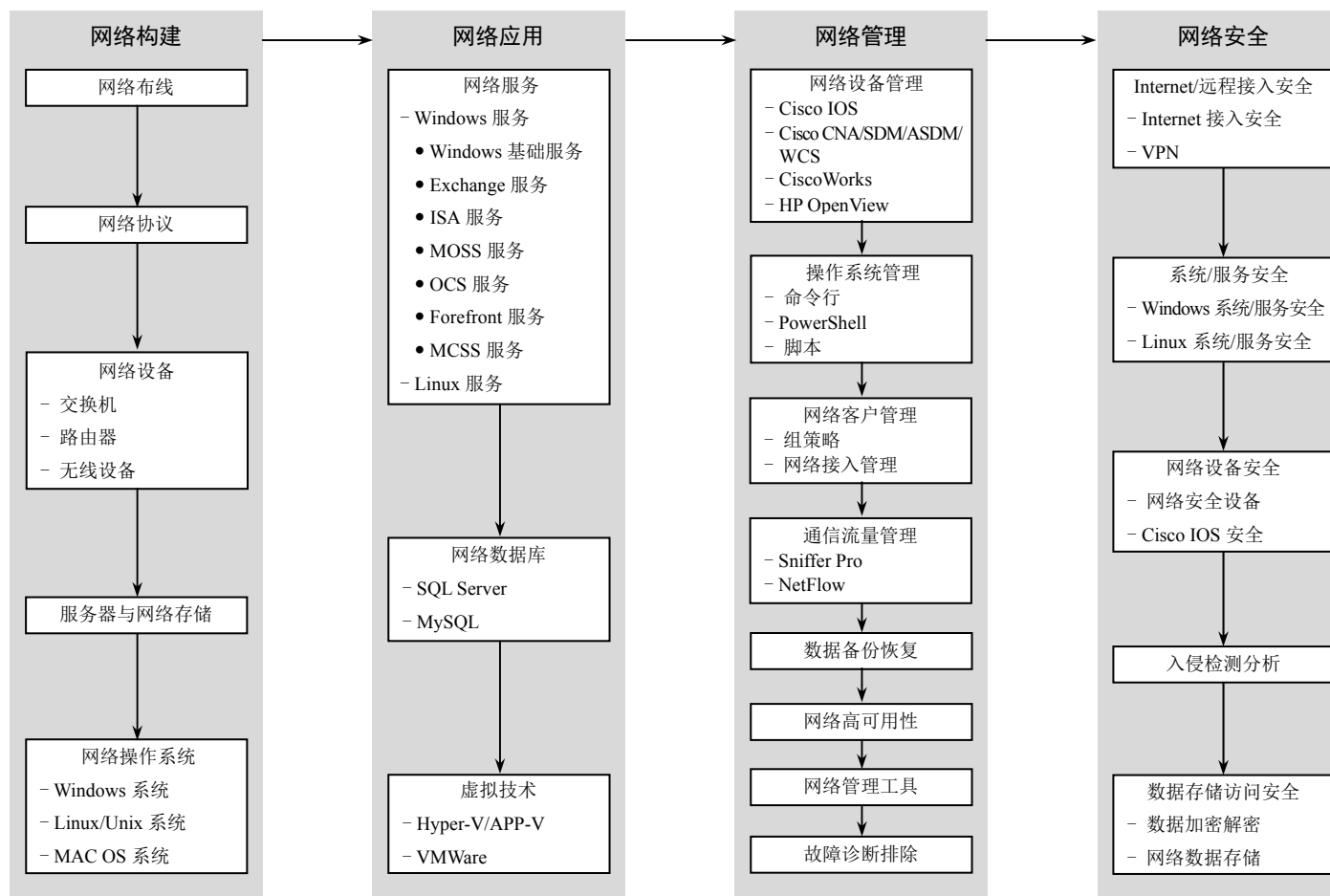
刘晓辉

2008.10



网管宝典学习路线图

笔者就自己对网络管理体系的理解，对网络管理学习者给出一个粗略线路图：





光盘说明

软硬件需要



硬件：PIII 500MHz 以上 CPU、256MB 以上内存、200MB 以上自由硬盘空间、支持 1024×768 分辨率的显卡和显示器、CD-ROM 或 DVD-ROM、声卡、音箱或耳机。



软件：Windows 98/2000/Me/2003/XP/Vista 操作系统，Macromedia Flash Player 6.0 以上播放器、设置 1024×768 分辨率。

操作指南



关闭所有正在运行的应用程序，将多媒体演示光盘置入光驱，光盘将自动运行并播放宣传片头动画，然后显示光盘名称界面（如图 1 所示），当出现鼠标时，在界面上单击，进入光盘章节界面（如图 2 所示）。

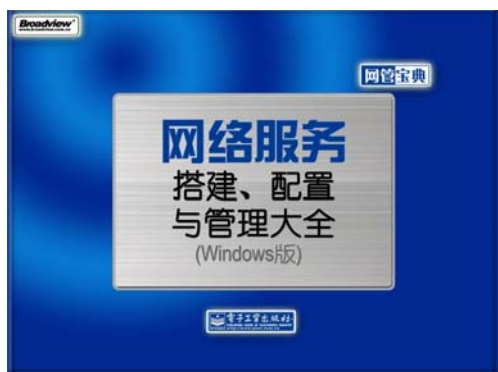


图 1 光盘名称界面



图 2 光盘章节界面



在光盘章节界面单击感兴趣的章节对应的按钮，进入要学习视频内容播放界面（如图 3 所示），视频自动播放，本光盘默认从第一视频开始播放。读者可以按照自己的需要调整解说和背景音乐的音量，并实现播放的暂停、快进、快退，也可以按下鼠标左键拖动视频播放滑块进行快速浏览，在播放条上单击，视频文件可以快速前进和后退。也可选择直接跳到下一个视频或返回上一个视频。



点击视频选择按钮，弹出视频选择界面（如图 4 所示），选择感兴趣的视频进行播放，具体操作与 Windows Media Player 非常相似。单击“返回”按钮，返回至光盘章节界面。



在光盘章节界面和播放界面中，单击“？”（光盘帮助）按钮，显示光盘使用帮助文件（如图 5 所示）。



单击“Exit”（退出光盘）按钮，显示光盘的制作团队信息（如图 6 所示），在退出界面上点击鼠标左键将自动结束光盘播放。

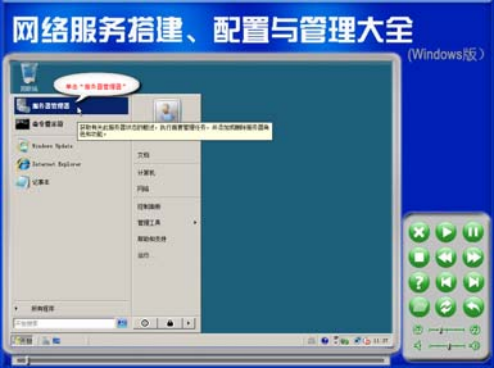


图3 视频内容播放界面



图4 视频选择界面



图5 光盘帮助



图6 退出界面

目 录

第 1 章 安装 Windows 服务器系统..... 1	
1.1 Windows 服务器系统概述..... 1	
1.1.1 Windows Server 2003 概述..... 1	
1.1.2 Windows Server 2008 概述..... 3	
1.2 安装 Windows Server 2003..... 6	
1.2.1 系统和硬件设备要求..... 6	
1.2.2 安装方式..... 7	
1.2.3 安装前注意事项..... 8	
1.2.4 安装 Windows Server 2003、SP 和 R2..... 9	
1.2.5 升级 Windows Server 2003..... 15	
1.2.6 添加与管理网络服务..... 18	
1.2.7 Windows Server 2003 控制台..... 20	
1.2.8 Windows Server 2003 系统设置..... 22	
1.3 安装 Windows Server 2008..... 25	
1.3.1 系统和硬件设备要求..... 25	
1.3.2 安装方式..... 26	
1.3.3 安装前注意事项..... 27	
1.3.4 安装 Windows Server 2008..... 27	
1.3.5 升级 Windows Server 2008..... 30	
1.3.6 添加与管理网络服务..... 32	
1.3.7 Windows Server 2008 控制台..... 34	
1.3.8 Windows Server 2008 系统设置..... 35	
第 2 章 Server Core..... 39	
2.1 概述..... 39	
2.1.1 Server Core 的优点..... 39	
2.1.2 Server Core 的缺点..... 39	
2.2 安装 Server Core..... 39	
2.2.1 安装 Server Core..... 40	
2.2.2 服务器关机..... 43	
2.3 重命名服务器..... 44	
2.4 设置 IP 地址..... 45	
2.5 安装 AD DS 域服务..... 45	
2.5.1 无人职守安装文件..... 46	
2.5.2 安装 AD DS 域服务..... 47	
2.6 安装服务组件..... 48	
2.6.1 启用远程管理..... 48	
2.6.2 客户端连接..... 49	
2.7 用户与组管理命令..... 50	
2.7.1 计算机账户管理——net computer..... 50	
2.7.2 用户账户管理——net user..... 50	
2.7.3 全局组管理——net group..... 53	
2.7.4 本地组管理——net localgroup..... 55	
2.7.5 身份识别工具——whoami..... 56	
2.8 AD DS 域服务管理命令..... 57	
2.8.1 添加目录对象工具——dsadd..... 57	
2.8.2 修改目录对象——dsmod..... 61	
2.8.3 删除目录对象——dsrm..... 67	
2.8.4 查询活动目录——dsquery..... 68	
第 3 章 配置与管理活动目录服务..... 77	
3.1 活动目录概述..... 77	
3.1.1 活动目录的重要意义..... 77	
3.1.2 活动目录对象..... 78	
3.1.3 活动目录组件..... 81	
3.1.4 活动目录结构..... 81	
3.1.5 复制活动目录..... 84	
3.1.6 命名规范..... 84	
3.2 安装与删除活动目录..... 85	
3.2.1 记录与设置服务器的相关参数..... 85	
3.2.2 安装域控制器和活动目录..... 86	
3.2.3 创建子域..... 90	
3.2.4 删除 Active Directory..... 93	
3.2.5 创建辅助域控制器..... 95	
3.3 备份与恢复活动目录..... 97	
3.3.1 备份系统状态..... 97	
3.3.2 恢复系统状态..... 102	
3.3.3 使用命令行工具..... 104	
3.4 拯救域控制器..... 108	
3.4.1 概述..... 108	
3.4.2 转移操作主机角色..... 108	
3.4.3 恢复原主域控制器..... 113	
3.4.4 占用操作主机角色..... 115	

3.5	域信任关系	118	5.3	配置与管理 DNS 服务器	159
3.5.1	信任关系	118	5.3.1	添加正向搜索区域	159
3.5.2	设置域信任关系	119	5.3.2	添加 DNS 区域	161
3.6	用户、组与组织单元	123	5.3.3	添加 DNS 记录	161
3.6.1	用户管理	123	5.3.4	添加反向查找区域	163
3.6.2	用户组管理	127	5.3.5	设置转发器	165
3.6.3	组织单位管理	130	5.3.6	添加辅助 DNS 服务器	166
3.7	组策略及其应用	131	5.3.7	备份 DNS 服务器信息	168
3.7.1	概述	131	第 6 章	配置与管理 DHCP 服务	169
3.7.2	组策略模板	132	6.1	DHCP 服务概述	169
3.7.3	通过组策略定制用户桌面	133	6.1.1	DHCP 服务简介	169
3.7.4	通过组策略安装应用程序	134	6.1.2	DHCP 工作原理	170
3.8	Windows 客户端加入域	138	6.1.3	DHCP 服务器授权	170
3.8.1	Windows 2000 Professional 用户	138	6.1.4	VLAN 与 DHCP 中继问题	171
3.8.2	Windows XP Professional 用户	139	6.2	安装 DHCP 服务器	171
3.8.3	Windows Vista 用户	141	6.2.1	安装 DHCP 服务器	171
第 4 章	WINS 服务	143	6.2.2	在 Active Directory 中授权	174
4.1	WINS 服务器概述	143	6.2.3	创建作用域	174
4.1.1	WINS 简介	143	6.2.4	创建保留地址	178
4.1.2	WINS 的工作机制	144	6.3	管理 DHCP 服务器	179
4.2	WINS 服务器的配置与管理	146	6.3.1	管理作用域	179
4.2.1	安装 WINS 服务器	146	6.3.2	备份与还原 DHCP 服务器	180
4.2.2	静态映射	146	6.3.3	迁移 DHCP 服务器	181
4.2.3	复制配置	148	6.3.4	跨网段的 DHCP 服务器	183
4.2.4	备份与还原 WINS 服务器	150	6.4	设置并使用 DHCP 客户端	187
4.3	设置 WINS 客户端	151	6.4.1	为 Windows 2000/XP 系统 启用 DHCP 客户端	187
4.3.1	在 DHCP 服务器中分配 WINS 服务器地址	151	6.4.2	为 Windows Vista 系统启用 DHCP 客户端	188
4.3.2	客户端配置	152	第 7 章	配置与管理打印服务	190
4.3.3	在自动获得 IP 地址的客户端 上验证	153	7.1	安装打印机服务器	190
第 5 章	配置与管理 DNS 服务	154	7.1.1	连接共享打印机	190
5.1	DNS 概述	154	7.1.2	安装打印服务器	191
5.1.1	DNS 系统结构	154	7.1.3	安装网络打印机	193
5.1.2	DNS 查询的工作过程与原理	155	7.1.4	管理打印机驱动程序	194
5.1.3	DNS 的反向查找	155	7.1.5	迁移打印服务器	196
5.1.4	DNS 转发器	156	7.2	管理打印服务器	198
5.1.5	动态更新	156	7.2.1	管理打印队列	198
5.1.6	活动目录集成	157	7.2.2	创建打印池	199
5.2	安装 DNS 服务器	157	7.2.3	设置打印机权限	200
5.2.1	安装活动目录的 DNS 要求	157	7.2.4	利用分隔页分隔打印文档	202
5.2.2	安装 DNS 服务	157	7.2.5	设置送纸器	203

7.2.6	管理等待打印的文档	203	8.8	Web 网站的远程管理	253
7.3	共享网络打印机	205	8.8.1	安装管理服务	253
7.3.1	安装打印机客户端	205	8.8.2	启用远程管理功能	254
7.3.2	安装 Web 共享打印机	206	8.8.3	创建 IIS 管理用户	256
7.3.3	使用浏览器连接到打印机	207	8.8.4	授权远程管理用户	258
7.3.4	使用“网上邻居”安装打印机	208	8.8.5	远程管理 Web 站点	259
第 8 章	配置与管理 Web 服务	210	8.9	Windows Server 2003/2008 的 配置差异	261
8.1	IIS 概述	210	第 9 章	配置与管理 FTP 服务	263
8.1.1	IIS 简介	210	9.1	FTP 服务概述	263
8.1.2	IIS 7.0	210	9.1.1	FTP 服务简介	263
8.2	搭建与管理 Web 服务	212	9.1.2	FTP 服务与 IIS	263
8.2.1	安装 Web 服务器	212	9.2	搭建与配置 FTP 服务器	263
8.2.2	配置 IP 地址和端口	216	9.2.1	安装 FTP 服务器	263
8.2.3	配置主目录	217	9.2.2	设置 IP 地址和端口号	266
8.2.4	配置默认文档	217	9.2.3	限制连接数量	266
8.2.5	配置访问权限和安全	218	9.2.4	设置主目录	267
8.2.6	配置自定义错误	222	9.2.5	设置欢迎和退出消息	267
8.2.7	配置 MIME 类型	223	9.2.6	设置访问安全	268
8.2.8	配置安全 Web 服务	224	9.2.7	设置用户访问权限	270
8.2.9	启动与停止 Web 服务器	226	9.2.8	启动与停止 FTP 服务器	273
8.3	创建与管理虚拟网站	226	9.3	创建与管理虚拟站点	273
8.3.1	虚拟网站概述	226	9.3.1	虚拟站点概述	273
8.3.2	虚拟网站创建方式	227	9.3.2	虚拟站点的创建方式	273
8.3.3	使用 IP 地址创建	228	9.3.3	使用 IP 地址创建	273
8.3.4	使用端口号创建	228	9.3.4	使用端口号创建	275
8.3.5	使用主机头名创建	229	9.3.5	管理虚拟站点	276
8.3.6	管理虚拟网站	230	9.4	创建与管理虚拟目录	276
8.4	创建与管理虚拟目录	230	9.4.1	虚拟目录概述	276
8.4.1	虚拟目录概述	230	9.4.2	虚拟目录的创建方式	277
8.4.2	虚拟目录创建方式	231	9.4.3	管理虚拟目录	278
8.4.3	管理虚拟目录	232	9.5	使用 Serv-U 搭建 FTP 服务器	278
8.5	安装与设置 Apache	232	9.5.1	搭建 Serv-U 服务器	278
8.5.1	安装 Apache	232	9.5.2	管理用户和权限	284
8.5.2	配置 Apache	234	9.5.3	管理域	288
8.6	搭建动态网站环境	236	9.6	使用 FTP 客户端	290
8.6.1	搭建 JSP 环境	236	9.6.1	访问 FTP 站点	290
8.6.2	搭建 CGI 环境	239	9.6.2	访问虚拟目录	292
8.6.3	搭建 ASP 环境	241	第 10 章	配置与管理文件服务	293
8.6.4	搭建 PHP 环境	243	10.1	文件共享与 NTFS 权限	293
8.7	安装与设置数据库	246	10.1.1	设置文件夹共享	293
8.7.1	安装与设置 MySQL	247	10.1.2	NTFS 权限	301
8.7.2	安装与设置 SQL Server	249			

10.1.3	设置 NTFS 权限	307	11.4.3	网站集管理	373
10.1.4	访问共享文件夹	310	11.5	通知管理	375
10.2	安装文件服务器	315	11.5.1	添加通知	375
10.3	分布式文件系统	320	11.5.2	编辑通知	376
10.3.1	特点及应用	321	11.5.3	删除通知	377
10.3.2	创建 DFS 映射	323	11.6	事件管理	378
10.3.3	DFS 复制	326	11.6.1	添加事件	378
10.4	磁盘配额	331	11.6.2	修改与删除事件	379
10.4.1	磁盘配额的功能	331	11.7	管理与使用链接	380
10.4.2	设置磁盘配额	331	11.7.1	添加链接	380
10.5	脱机文件与数据同步	334	11.7.2	编辑链接	381
10.5.1	设置服务端的脱机文件	334	11.7.3	删除链接	382
10.5.2	Windows XP/2003 客户端的 脱机文件设置与同步	335	11.7.4	修改链接 Web 部件	382
10.5.3	Windows Vista/2008 客户端 脱机文件的加密与同步	337	11.8	使用文档库	383
10.6	实现软 RAID	339	11.8.1	创建文档库	383
10.6.1	卷与 RAID	339	11.8.2	修改和使用文档库	384
10.6.2	动态磁盘	343	11.8.3	直接从 Word 中发布文档库	386
10.6.3	实现软 RAID	345	11.9	使用列表	388
11.1	办公自动化系统概述	348	11.9.1	创建列表	389
11.1.1	WSS 服务器要求	348	11.9.2	修改列表	390
11.1.2	解决方案	348	11.9.3	在 Excel 中直接发布列表	391
11.2	安装与配置服务器端	349	11.10	使用 Microsoft 提供的 WSS 模板	392
11.2.1	安装前的准备	349	11.10.1	WSS 模板功能	392
11.2.2	安装 WSS	349	11.10.2	上传模板到 WSS 网站	393
11.2.3	框架生成与基本功能	352	11.10.3	使用 WSS 模板创建站点	395
11.3	基于 WSS 的办公自动化系统 细节设置	354	11.11	Windows Server 2003 R2/2008 的配置差异	395
11.3.1	办公自动化站点的用户管理	354	12.1	电子证书和认证服务概述	396
11.3.2	管理网站和工作区	356	12.1.1	数字证书简介	396
11.3.3	配置网站和创建工作区	357	12.1.2	认证服务简介	396
11.3.4	更改网站标题和说明	358	12.2	电子证书服务	397
11.3.5	修改网站主题	359	12.2.1	安装企业 CA	397
11.3.6	自定义主页	359	12.2.2	安装独立根 CA	403
11.3.7	修改当前登录用户信息	361	12.3	使用企业证书服务	404
11.3.8	修改当前用户的通知	363	12.3.1	使用 Web 方式申请与安装证书	404
11.3.9	查看网站用户的信息	365	12.3.2	使用“证书申请向导”申请 证书	409
11.4	WSS 网站管理	365	12.3.3	导出与导入证书	412
11.4.1	管理用户和权限	366	12.4	使用独立证书服务	415
11.4.2	网站管理	368	12.4.1	申请证书	415

12.4.2	颁发证书	418	14.2.4	其他考虑事项	463
12.4.3	在客户端安装证书	418	14.2.5	远程安装服务的前期准备	463
12.5	备份与还原证书服务器	420	14.3	RIS 远程安装服务实现步骤	463
12.5.1	备份证书	420	14.3.1	安装 RIS 服务器	464
12.5.2	还原证书	420	14.3.2	授权 RIS 服务器	466
12.6	管理证书服务	422	14.3.3	配置 RIS 服务器	467
12.6.1	吊销证书	422	14.3.4	禁止 RIS 安装过程中重新分区 硬盘	468
12.6.2	解除吊销的证书	422	14.3.5	自动完成 RIS 远程安装系统	470
12.6.3	证书续订	422	14.3.6	允许远程安装	471
12.7	配置安全 Web 服务器	424	14.3.7	委派所有用户可以将计算机 加入到域	472
12.7.1	为 Web 服务器申请证书	424	14.4	实现远程安装服务	473
12.7.2	将证书应用于 Web 服务器	429	14.4.1	远程安装对客户端的需求	473
12.7.3	在工作站上验证 Web 服务器	429	14.4.2	创建引导软盘	473
12.8	Windows Server 2003/2008 的 配置差异	430	14.4.3	在客户端中安装 Windows XP Professional	474
第 13 章	配置与管理终端服务	432	14.5	安装与配置 Windows 部署服务	476
13.1	安装终端服务	432	14.5.1	Windows 部署服务组件	477
13.1.1	终端服务概述	432	14.5.2	Windows 部署服务的优点	477
13.1.2	虚拟化	433	14.5.3	服务器的功能模式	477
13.1.3	安装终端服务	434	14.5.4	Windows 部署服务的要求	478
13.1.4	终端服务器授权	439	14.5.5	安装 Windows 部署服务	478
13.2	远程桌面连接	441	14.5.6	启动 Windows 部署服务	480
13.2.1	在 Windows 9x/2000 客户端上 远程管理	441	第 15 章	配置与管理系统更新服务	483
13.2.2	在 Windows XP/2003/Vista/2008 客户端上远程管理	443	15.1	WSUS 3.0 概述与系统需求	483
13.3	使用 Web 方式远程管理	445	15.1.1	WSUS 概述	483
13.3.1	安装远程桌面 Web 连接组件	445	15.1.2	WSUS 3.0 系统需求	483
13.3.2	使用 IE 远程管理	451	15.1.3	文件系统需求	484
13.4	应用程序虚拟化	454	15.1.4	WSUS 的体系结构	484
13.4.1	发布应用程序	454	15.1.5	客户端自动更新要求	485
13.4.2	创建 RDP 文件	455	15.2	安装与配置 WSUS 3.0	485
13.4.3	访问应用程序	456	15.2.1	全新安装 WSUS 3.0 服务器的 准备	485
第 14 章	配置与管理远程安装服务	461	15.2.2	安装 WSUS 服务器	488
14.1	远程安装服务与 Windows 部署 服务概述	461	15.2.3	WSUS 3.0 配置向导	490
14.1.1	远程安装服务简介	461	15.3	配置客户端	494
14.1.2	Windows 部署服务简介	461	15.3.1	安装 WSUS 客户端	494
14.2	远程安装服务的系统需求	462	15.3.2	通过本地策略配置客户端	494
14.2.1	服务需求	462	15.4	配置 WSUS 服务器	496
14.2.2	服务器硬件需求	462	15.4.1	WSUS 的更新设置	497
14.2.3	客户端需求	463	15.4.2	WSUS 服务器中的计算机分组	500
			15.4.3	同步	503

15.4.4	报告	503	17.2.3	配置 AD RMS 服务器	562
15.5	WSUS 服务器的选项	508	17.3	安装和配置 AD RMS 客户端	579
15.5.1	更新源和代理服务器设置	508	17.3.1	安装客户端	580
15.5.2	产品和分类	509	17.3.2	使用 RMS 保护文档	580
15.5.3	更新文件和语言	509	17.3.3	受限客户端应用被保护文档	583
15.5.4	同步计划	509	17.3.4	应用 RMS Toolkit	584
15.5.5	自动审批	510	17.3.5	应用非常规客户端	586
15.5.6	分组计算机	512	第 18 章	MOM 管理服务器	587
15.5.7	服务器清理向导	512	18.1	MOM 概述	587
15.5.8	报告汇总	513	18.1.1	监控模式	587
15.5.9	电子邮件通知	513	18.1.2	MOM 服务器	587
15.5.10	WSUS 服务器配置向导	514	18.1.3	MOM 数据库	587
第 16 章	网络策略和访问服务	515	18.1.4	报表服务	588
16.1	路由和远程访问服务简介	515	18.2	安装 MOM	588
16.1.1	远程访问服务器概述	515	18.2.1	安装 MOM 前的准备工作	588
16.1.2	NAP 概述	516	18.2.2	安装 Microsoft Operations Manager 2005 组件	590
16.1.3	VPN 服务概述	517	18.2.3	安装 Microsoft Operations Manager 2005 报表	593
16.2	配置和管理远程访问服务	518	18.3	安装代理	596
16.2.1	配置准备工作	518	18.3.1	计算机发现规则	596
16.2.2	配置远程访问服务	521	18.3.2	安装代理服务	598
16.2.3	设置 VPN 服务器	526	18.4	安装管理包	601
16.2.4	配置远程访问服务客户端	534	18.4.1	下载管理包	601
16.3	配置 NPS 策略	537	18.4.2	导入 Active Directory 管理包	604
16.3.1	配置网络健康验证器	537	18.4.3	导入 Microsoft SQL Server 管理包	605
16.3.2	配置更新服务器组	539	18.5	计算机组	605
16.3.3	配置健康策略	540	18.5.1	创建自定义组	606
16.3.4	配置网络策略	541	18.5.2	设置计算机组成员	609
16.4	配置 NPS 客户端	547	18.6	规则组	609
16.4.1	启用安全中心	547	18.6.1	创建规则组	610
16.4.2	配置 NAP 客户端	548	18.6.2	创建事件规则	612
16.4.3	配置 NAP 代理服务	550	18.6.3	创建警报规则	614
16.5	Windows Server 2000/2003 的 配置差异	551	18.6.4	创建性能规则	615
第 17 章	AD RMS 服务	552	18.6.5	关联规则组和计算机组	617
17.1	AD RMS 概述	552	18.7	任务	618
17.1.1	AD RMS 的新特性	552	18.7.1	创建任务	618
17.1.2	AD RMS 的相关组件	552	18.7.2	编辑任务	620
17.1.3	AD RMS 的实现原理	553	18.8	通知	620
17.1.4	AD RMS 服务器的软件需求	554	18.8.1	创建通知组	620
17.2	AD RMS 服务器的安装和配置	554	18.8.2	关联操作员到通知组	622
17.2.1	准备工作	554	18.9	操作员控制台	622
17.2.2	安装 AD RMS 根服务器	554			

18.9.1 处理警报	622	19.7.1 启用缓存	667
18.9.2 图示	626	19.7.2 创建正向缓存	668
18.9.3 事件	626	19.7.3 禁止反向缓存	670
18.9.4 状态	627	19.7.4 禁止缓存某些站点	671
18.9.5 性能	628	19.8 备份与恢复 ISA Server 2006	671
18.9.6 计算机和组	629	19.8.1 备份防火墙策略	672
18.9.7 任务	631	19.8.2 备份 ISA Server 2006 的所有 配置	673
第 19 章 配置与管理 ISA 服务	633	19.8.3 恢复 ISA Server 2006 的配置	673
19.1 ISA Server 2006 概述	633	第 20 章 配置与管理网络防病毒服务	675
19.1.1 ISA Server 2006 功能简介	633	20.1 安装 Symantec Endpoint Protection 企业版	675
19.1.2 ISA Server 2006 中的网络	634	20.1.1 Symantec 产品简介	675
19.1.3 ISA Server 2006 的客户端	634	20.1.2 安装 Symantec Endpoint Protection Manager	678
19.2 应用 ISA Server	635	20.2 部署 Symantec Endpoint Protection 客户端	686
19.2.1 Internet 边缘防火墙	635	20.2.1 部署受管理客户端	686
19.2.2 部门或主干网络防火墙	635	20.2.2 部署非受管客户端	691
19.2.3 分支办公室防火墙	635	20.3 升级病毒库	693
19.2.4 发布安全服务器	635	20.3.1 安装 LiveUpdate 管理工具	693
19.3 部署 ISA Server 2006	636	20.3.2 配置更新	694
19.3.1 安装 ISA Server 2006 的软件与 硬件需求	636	20.3.3 配置 LiveUpdate 策略	702
19.3.2 安装 ISA Server 2006	636	第 21 章 流媒体服务	705
19.4 实现安全 Internet 共享	640	21.1 流媒体服务的安装	705
19.4.1 允许内网访问 Internet	640	21.1.1 流媒体概述	705
19.4.2 允许内网 ping 通网关	644	21.1.2 流媒体传输协议	705
19.4.3 设置 Internet 访问限制	645	21.1.3 点播与广播	706
19.4.4 设置屏蔽网站	649	21.1.4 Windows Media 服务的安装	706
19.4.5 设置阻止文件类型	651	21.2 实现点播和广播	708
19.4.6 设置用户分组与权限	651	21.2.1 实现视频和音频点播	708
19.5 发布内部服务器	652	21.2.2 实现视频和音频广播	712
19.5.1 发布 Web 站点	652	21.2.3 制作播放列表	713
19.5.2 发布邮件服务器	656	21.2.4 发布广告	715
19.5.3 发布 Exchange Web 客户端访问	657	21.2.5 对点播发布点的访问	716
19.5.4 发布 SharePoint 站点	659	第 22 章 Exchange Server 2007 邮件 服务	718
19.5.5 发布其他服务器	660	22.1 Exchange Server 2007 的系统 需求	718
19.5.6 发布安全 Web 服务器	661	22.1.1 硬件需求	718
19.5.7 为 Internet 用户提供代理服务	661	22.1.2 软件需求	718
19.6 实现安全 VPN 访问服务	664		
19.6.1 在 ISA Server 中启用 VPN 服务器	664		
19.6.2 检查与配置 VPN 服务器	666		
19.6.3 管理与设置用户	666		
19.7 高效访问 Internet	667		

22.2	安装 Exchange Server 2007	718	23.3.1	设置 IP 地址	752
22.2.1	升级到 Active Directory 服务器	719	23.3.2	在域控制器上准备 OCS 架构	753
22.2.2	安装相关组件	719	23.3.3	部署 OCS 2007	757
22.2.3	安装 Exchange Server 2007 SP1	721	23.3.4	在 OCS 服务器上配置 TCP	766
22.3	配置 Exchange Server 2007	723	23.3.5	创建域用户	768
22.3.1	部署“所有 Exchange 服务器”	723	23.3.6	配置 OCS 的用户账户	768
22.3.2	配置脱机通信簿及公用文件夹 分发	724	23.4	OCS 2007 客户端	768
22.3.3	“客户端访问”的部署	725	23.4.1	OCS 2007 客户端的新增功能	769
22.3.4	部署“集线器传输”	728	23.4.2	部署 OCS 2007 客户端	770
22.3.5	设置默认用户邮箱大小	734	23.4.3	OCS 的应用	776
22.3.6	设置单个邮件大小	734	23.5	Live Meeting 2007 的部署与应用	777
22.3.7	HELO 信息设置	736	23.5.1	部署 Live Meeting 2007	777
22.3.8	公用文件夹设置	737	23.5.2	Live Meeting 2007 客户端的应用	778
22.4	用户管理	739	23.6	Outlook 会议外接程序	780
22.4.1	同时创建用户和邮箱	739	23.6.1	配置 Outlook 的会议外接程序	780
22.4.2	为已有用户创建邮箱	741	23.6.2	创建会议并加入会议	781
22.4.3	通信组设置	741			
22.4.4	用户属性	743	第 24 章	Hyper-V	784
22.5	客户端的使用	744	24.1	Hyper-V 概述	784
22.5.1	Outlook 2003/Office 2007 的使用	745	24.1.1	Hyper-V 系统需求	784
22.5.2	OWA 的使用	748	24.1.2	Hyper-V 优点	784
第 23 章	OCS 2007 即时消息服务	749	24.2	安装与配置 Hyper-V	785
23.1	OCS 2007 简介	749	24.2.1	安装 Hyper-V 角色	785
23.1.1	OCS 2007 组件	749	24.2.2	配置 Hyper-V 服务器	787
23.1.2	OCS 服务模板	750	24.2.3	配置虚拟机	792
23.2	OCS 2007 需求	751	24.3	创建虚拟网络	796
23.2.1	OCS 2007 的硬件要求	751	24.4	创建虚拟磁盘	798
23.2.2	OCS 2007 支持的操作系统及 环境需求	751	24.4.1	创建虚拟磁盘	798
23.2.3	Windows 服务依赖项	752	24.4.2	配置虚拟磁盘	799
23.3	部署 OCS 2007	752	24.5	创建虚拟机	801
			24.5.1	创建虚拟机	801
			24.5.2	配置虚拟机属性	802
			24.5.3	安装虚拟机操作系统	805

第 1 章 安装 Windows 服务器系统

服务器相当于网络的“大脑”，用来为网络提供各种各样的服务并控制网络的运行。服务器的运行离不开操作系统的支持，目前常用的服务器操作系统有 Windows、Linux 和 Unix。其中 Windows 系统以其简单易用的特点，受到广大中小型企业青睐，广泛应用于各中小型网络中。

1.1 Windows 服务器系统概述

为了保证服务器能够稳定且高效地运行，首先要选择一个稳定、易用且功能强大的操作系统。微软推出的 Windows Server 系统一向秉承简单易用的风格，占领了中小企业的大部分市场，是中小型网络应用服务器的首选。尤其是 Windows Server 2008 系统，不仅更加简单易用，而且无论是功能，还是性能，都有极大的提升。

1.1.1 Windows Server 2003 概述

Windows Server 2003 继承了 Windows 2000 Server 的核心技术，而且更加稳定、安全且易于操作。它可以在任意规模的企业中充当理想的服务器平台，从而提高企业和员工的工作效率，实现彼此之间更好的沟通。因此推出后迅速取代后者而成为主流的服务器操作系统，图 1-1 所示为 Windows Server 2003 的启动界面。



图 1-1 Windows Server 2003 的启动界面

1. Windows Server 2003 的特点

Windows Server 2003 操作系统继承和发扬了 Windows 2000 Server 技术中的精华，并且使其更加易于部署、管理和使用，从而为企业网络实现了一个高效的基础架构。而 Windows Server 2003 R2 更是扩展了 Windows Server 2003，带来了活动目录、存储和分支机构方面的增强功能，增强了对资源的管理和控制。Windows Server 2003 主要具有以下特点。

(1) 综合性能高

Windows Server 2003 操作系统具有高可靠性、实用性、可伸缩性和安全性，主要表现在以下几个方面。

实用性：增强了对群集的支持，提供了更强的故障转移能力和更长的系统运行时间。如果集群中某个节点由于故障或者维护而不能使用，另一节点会立即提供服务。而网络负载均衡（NLB）

功能可以在群集的各个节点之间平衡 IP 通信。

可伸缩性：借助对称多处理技术（SMP）可以增加处理器，借助群集技术则可将多台服务器有机地连接在一起，从而拥有非常高的可伸缩性。

安全性：由于 Intranet、Extranet 和 Internet 站点的结合，系统安全问题也比以往任何时候都更为严峻。Windows Server 2003 提供了许多重要、安全及改进的功能，提高了系统可靠性，降低了缺陷数量，减少了由常见的编程错误引起的安全漏洞，并集成了可提高 Web 服务器的安全性和性能的 Internet 信息服务（IIS 6.0）。

（2）优秀的网络服务

Windows Server 2003 提供了许多优秀的网络服务，可以提高企业和员工的工作效率、主要包括以下方面。

文件和打印服务器：Windows Server 2003 提供了智能的文件和打印服务。性能和功能都得到很大程度的提高，可以有效地降低企业总拥有成本。

活动目录：即 Active Directory，其中存储了网络上的几乎所有对象的信息，并且通过提供目录信息的逻辑分层组织，使管理员和用户易于找到该信息。Windows Server 2003 的活动目录更通用、更可靠、更经济，并且性能和可伸缩性更高，可以更加灵活地设计、部署和管理企业的目录。

管理服务：随着计算机数量的不断增加，维护成本也随之增加。通过自动化来减少日常维护，无疑是降低成本的关键。Windows Server 2003 提供了多套重要的自动管理工具，如 Windows 服务器更新服务（WSUS）和服务器配置向导。新的组策略管理控制台（GPMC）使得管理组策略更加容易，从而可以更好地利用活动目录服务及其强大的管理功能。

存储管理：Windows Server 2003 在管理及维护磁盘和卷、备份和恢复数据，以及连接存储区域网络（SAN）更为简易和可靠。

终端服务：利用终端服务可以在网络中的任何一台计算机远程管理服务器及设备，如同位于服务器面前一样，从而方便了管理员的操作。

（3）稳定的连接状态

Windows Server 2003 的许多新功能和改善措施可确保企业和用户保持稳定的连接状态，主要表现在以下方面。

XML Web 服务：IIS 6.0 极大地提高了可靠性、可伸缩性和性能。默认情况下，它以锁定状态安装。管理员根据需要来启用或禁用系统功能，从而提高了安全性。此外，还增强了对直接编辑 XML metabase 数据库的管理。

网络和通信：员工需要在任何地点并使用任何设备接入网络，合作伙伴、供应商和分支机构需要与关键资源进行高效地相互沟通，而且安全性比以往任何时候都重要。Windows Server 2003 扩展了网络结构的多功能性、可管理性和可靠性。

企业 UDDI（通用描述发现和集成）服务：这是用于发布和查找有关 Web 服务的信息的工业规范。UDDI 服务是 XML Web 服务的动态而灵活的架构，可使企业能够运行自己的内部 UDDI 服务。从而生成和部署更智能且更可靠的应用程序，以供 Intranet 和 Extranet 使用。

Windows 媒体服务：Windows Server 2003 内置了强大的数字流媒体服务——Windows Media 服务，包括 Windows 媒体播放器、Windows 媒体编辑器、音频/视频编码解码器，以及 Windows 媒体软件开发工具包。

（4）经济性

Windows Server 2003 提供了简单易用的说明指南，为各种技术的使用提供了完整的解决方案。通过利用最新的硬件、软件和方法来优化服务器部署可以降低用户的总拥有成本，从而使用户的投资快速得到回报。

随着 Intel 和 AMD 64 位处理器的推出与普及, Windows Server 2003 成为中低端 IA 架构服务器的首选。对于那些没有经过 Linux 和 Unix 培训的系统管理员而言, Windows Server 2003 更容易部署和使用。

2. Windows Server 2003 的版本

Windows Server 2003 有 4 个不同的版本, 即 Windows Server 2003 标准版 (Standard Edition)、Windows Server 2003 企业版 (Enterprise Edition)、Windows Server 2003 数据中心版 (Datacenter Edition) 和 Windows Server 2003 Web 版 (Web Edition)。这些版本支持不同的硬件设备, 拥有不同的性能, 并且提供不同的网络服务, 用户可以根据自己的网络需求选择。

(1) Windows Server 2003 标准版

Windows Server 2003 标准版是一个可靠的网络操作系统, 可迅速方便地提供企业解决方案, 这种灵活的服务器是小型企业和部门应用的理想选择。该版本支持 4 个处理器, 主要用于提供文件和打印机共享, 以及安全的 Internet 连接, 并且允许集中化的桌面应用程序部署。需要注意的是, 该版本不支持服务器集群。

(2) Windows Server 2003 企业版

Windows Server 2003 企业版为满足各种规模的企业的一般用途而设计, 是一种全功能的服务器操作系统。它提供高度可靠性、高性能和出色的商业价值, 是构建各种应用程序、Web 服务和基础结构的理想平台。该版本可基于 Intel Itanium 系列计算机, 支持 8 个 CPU 和 64 位计算平台。它在功能上与标准版基本相同, 只是提供了对更高硬件系统的支持。因此可用于更大规模的网络, 支持更多数量的用户和更复杂的网络应用。

(3) Windows Server 2003 数据中心版

Windows Server 2003 数据中心版是为运行企业和任务所倚重的应用程序而设计的, 是功能最强大的版本。它支持高达 32 路的 SMP 和 64 GB 的 RAM, 提供 8 节点群集和负载平衡服务是其标准功能, 可用于能够支持 64 位处理器和 512 GB RAM 的 64 位计算平台。

(4) Windows Server 2003 Web 版

Windows Server 2003 Web 版是 Windows 系列中的新产品, 主要目的是作为 IIS 6.0 Web 服务器使用。它用于生成和承载 Web 应用程序、Web 页面, 以及 XML Web 服务。并且提供一个快速开发和部署 XML Web 服务和应用程序的平台, 以实现 Web 服务和托管。与标准版相同, 该版本也不支持服务器集群。

1.1.2 Windows Server 2008 概述

Windows Server 2008 是微软公司全力打造的新一代服务器操作系统, 虽然基于 Windows Server 2003 开发, 但无论是从实用性、安全性, 还是可操作性方面都有了质的飞跃。它可以更加充分地发挥服务器的硬件性能, 为企业网络提供更高效的网络传输和更可靠的安全管理。不仅减轻了管理员部署的负担, 而且提高了工作效率, 降低了成本。

1. Windows Server 2008 简介

Windows Server 2008 操作系统不仅保留了 Windows Server 2003 的所有优点, 还引进了多项新技术, 如虚拟化应用、网络负载均衡及网络安全服务等。图 1-2 所示为 Windows Server 2008 桌面。

Windows Server 2008 主要具有以下特点。

(1) 更强的控制能力: Windows Server 2008 作为网络服务器平台, 使网络管理员可以更好地控制服务器和网络基础结构, 从而将精力放在处理关键业务需求上。例如, 增强的脚本编写和任务自动化功能 (如 Windows PowerShell) 可帮助网络管理员自动执行常见任务, “服务器管理器” 可以集中安装和配置服务角色及功能等。



图 1-2 Windows Server 2008 桌面

(2) 可靠的网络安全性: Windows Server 2008 提供了一系列新的和改进的安全技术, 增强了对操作系统的保护, 为企业的运营和发展奠定了坚实的基础。通过提供减小内核攻击面的安全创新思路(例如 PatchGuard)使服务器环境更安全且更稳定。这些技术包括网络访问保护(NAP)、只读域控制器(RODC)、公钥基础结构(PKI)增强功能、Windows 服务强化、双向 Windows 防火墙和新一代加密支持等。

(3) 更大的灵活性: Windows Server 2008 允许管理员修改其基础结构, 以适应不断变化的业务需求。并且允许用户从远程位置(如远程应用程序和终端服务网关)执行程序, 为移动工作人员增强了灵活性。而 Windows 部署服务则加快了客户端系统的部署和维护, 使用 Windows Server 虚拟化(WSv)可帮助合并服务器。

2. Windows Server 2008 新功能

Windows Server 2008 操作系统中增加了许多新功能, 相对于 Windows Server 2003 而言更易用、更稳定、更安全且更强大。这些新功能如下。

(1) IIS 7.0

Windows Server 2008 操作系统绑定了 IIS 7.0, 相对于 IIS 6.0 而言, 是最具飞跃性的升级产品。通过委派管理、增强的安全性和缩小的攻击面、Web 服务的集成应用程序, 以及改进的管理工具等关键功能提高了安全性和管理性。例如, Web 站点的管理权限更加细化, 可以将各种操作权限委派给指定的管理员, 从而极大地优化了网络管理。

(2) 虚拟化(WSv)

通过 Windows Server 2008 内置的服务器虚拟技术, 可以在单台服务器上虚拟 Windows 及 Linux 等多个操作系统, 并与现有环境互操作。利用更加简单且灵活的授权策略可以更容易地利用虚拟化的各种优势。同时也可以节省成本、提高硬件使用率、优化基础结构并提高服务器可用性。

(3) 服务器核心(Server Core)

Windows Server 2008 提供了 Server Core 功能, 这是一个不包含服务器图形用户界面的操作系统。和 Linux 操作系统一样, 只安装必要的服务和应用程序, 并且只提供基本的服务器功能。由于服务器上安装和运行的程序和组件较少, 暴露在网络上的攻击面也较少, 因此更加安全, 通常只需要较少的维护和更新。

(4) 网络访问保护(NAP)

网络访问保护允许网络管理员自定义网络要求, 并限制不符合这些要求的计算机访问网络。NAP 强制执行管理员定义的正常策略, 这些策略包括连接网络的计算机的软件要求、安全更新要求和

所需的配置设置等内容。

NAP 强制实现方法支持 4 种网络访问技术，与 NAP 结合使用来强制实现正常运行的策略，包括 Internet 协议安全（IPsec）强制、802.1X 强制、用于路由和远程访问的虚拟专用网络（VPN）强制，以及动态主机配置协议（DHCP）强制。

（5）只读域控制器（RODC）

这是 Windows Server 2008 操作系统提供的一种新类型的域控制器，可以在域控制器安全性无法保证的位置轻松部署域控制器，从而降低了在无法保证物理安全的远程位置（如分支机构）中部署域控制器的风险。RODC 维护 Active Directory 目录服务数据库的只读副本，通过将该数据库副本放置在更接近分支机构的地方，使用户可以更快地登录。即使身处没有足够物理安全性来部署传统域控制器的环境，也能更有效地访问网络中的身份验证资源。

（6）Windows PowerShell

这是一种新的命令行 Shell，包含 130 多种工具和一种集成的脚本语言。使网络管理员能够更轻松的控制并更安全地自动执行日常系统管理任务，在跨多台服务器的情况下尤其有用。Windows PowerShell 不需要迁移现有脚本，可以自动化执行系统管理任务（如 Active Directory、终端服务器及 IIS 7.0），从而提高了组织解决其环境特有的系统管理问题的能力。

Windows PowerShell 不需要编程背景，使用现有的 IT 基础结构、脚本和命令行工具即可，因此非常易于学习和使用。

（7）Windows 防火墙高级安全功能

Windows 防火墙可以据其配置和当前运行的应用程序来允许或阻止网络通信，从而保护网络免遭恶意用户和程序的入侵。并且防火墙的这种功能是双向的，即可以同时传入和传出的通信进行拦截。在 Windows Server 2008 中已经配置了系统防火墙专用的 MMC 控制台单元，可以通过远程桌面或终端服务等实现远程管理和配置。

（8）BitLocker 驱动器加密

BitLocker 驱动器加密是 Windows Server 2008 中一个重要的新功能，可保护服务器、工作站和移动计算机。BitLocker 可对磁盘驱动器的内容加密，防止未经授权的使用者绕过文件和系统保护，或者对存储在受保护驱动器中的文件进行脱机查看。

（9）下一代加密技术（Cryptography Next Generation, CNG）

CNG 加密技术提供了灵活的加密开发平台，允许 IT 专业人员在与加密相关的应用程序（如 Active Directory 证书服务、安全套接字层（SSL）和 Internet 协议安全（IPsec））中创建、更新和使用自定义加密算法。

（10）增强的终端服务

Windows Server 2008 的终端服务包含新增的核心功能，改善了最终用户连接到 Windows Server 2008 终端服务器时的体验。Terminal Services RemoteApp 将终端服务器中运行的应用程序与用户桌面完全集成，允许远程用户访问在本地计算机硬盘上运行的应用程序。和终端服务安全网关一起应用，使用户通过 HTTPS 访问远程桌面和远程应用程序，而不受防火墙的限制。

（11）服务器管理器

服务器管理器是 Windows Server 2008 的一个新功能，它将 Windows Server 2003 的许多功能替换合并在一起，如“管理您的服务器”、“配置您的服务器”、“添加或删除 Windows 组件”和“计算机管理”等，使得管理更加方便。

3. Windows Server 2008 版本

Windows Server 2008 具有标准版、企业版、数据中心版和安腾版 4 个版本，并分别有 32 位和 64 位版本。这些版本可以适应不同企业的需求和系统环境，从小型企业到全球性的大型分布式网络环境都可以找到适合自己的产品：

(1) Windows Server 2008 标准版

Windows Server 2008 标准版是一个可靠的网络操作系统，可迅速方便地提供企业解决方案。强大的网络部署和管控功能节约了用户大量的财力和人力资源，这种灵活的服务器是小型企业和部门应用的理想选择。该版本具备了大多数网络需要的基本网络功能和全能的 Server Core 安装选项，通常用于提供文件和打印机共享及 Internet 安全连接等，并允许集中化的桌面应用程序部署。Windows 2008 Server X86 标准版最大可支持 4 GB 内存和 4 路处理器，而 64 位标准版则最大可支持 64 GB 内存。

(2) Windows Server 2008 企业版

Windows Server 2008 企业版为满足各种规模的企业的一般用途而设计，是一种全功能的服务器操作系统。它提供高度可靠性、高性能和出色的商业价值，是构建各种应用程序、Web 服务和基础结构的理想平台。该版本在功能类型上与标准版基本相同，只是提供了对更高硬件系统的支持，同时提供了更加优良的可伸缩性和可用性。并且在原基础上添加了企业技术，例如 Failover Clustering 与活动目录联合服务等。32 位企业版最多可支持 8 路处理器和 64 GB 内存，而 64 位企业版最大可支持 2 TB 内存。Windows Server 2008 企业版可用于更大规模的网络，支持更多数量的用户和更复杂的网络应用。

(3) Windows Server 2008 数据中心版

Windows Server 2008 数据中心版是为运行企业和任务所倚重的应用程序而设计的，这些应用程序需要最高的可伸缩性和可用性，是 Microsoft 迄今为止开发的功能最强大的服务器操作系统。它支持高达 32 路的 SMP 和 64 GB 的 RAM，提供 8 节点群集和负载平衡服务是它的标准功能。64 位数据中心版则最大可支持 2 TB 内存，更加方便了企业网络服务性能优化和升级。另外，该版本还可以提供无限量的虚拟镜像应用。

(4) Windows Server 2008 安腾版

Windows Server 2008 安腾版是专为 Intel Itanium 64 位处理器设计，可以提供 Web 和应用程序服务器功能。根据平台支持的不同，部分角色和功能可能无法正确运行。该版本最高可支持 2 TB 内存。

提示 以上介绍的 4 个版本均支持 Server Core 安装技术和虚拟化技术，除 Windows Server 2008 安腾版外，其他 3 个版本均不支持虚拟化技术。

1.2 安装 Windows Server 2003

Windows Server 2003 虽然是服务器操作系统，但完全可以利用向导安装，同时可以完成分区格式化、授权及设置网络信息等功能。在安装完成后，则可配置网络协议、自动更新并使用安全配置向导等。

1.2.1 系统和硬件设备要求

Windows Server 2003 对服务器硬件有一定的要求，而且不同版本的操作系统对服务器的需求也不一样。表 1-1 所示为 Windows Server 2003 系统对服务器硬件的基本需求和推荐配置。

表 1-1 Windows Server 2003 的硬件需求

		标准版	企业版	数据中心版
基本需求	处理器	133 MHz 处理器	133 MHz 处理器	400 MHz 处理器
	内存	128 MB	128 MB	512 MB
	磁盘空间	1.25 GB 可用空间	1.25 GB 可用空间	1.5 GB 可用空间
	其他	无	无	8 路对称式多处理器
推荐配置	处理器	550 MHz，最多可支持 4 处理器	550 MHz，最多可支持 8 处理器	733 MHz 或更高处理器
	内存	256 MB，最多支持 4GB	256 MB，最多支持 64GB	1 GMB，最多支持 128 GB
	磁盘空间	2 GB 或更多	2 GB 或更多	3 GB 或更多
	其他	无	无	最多可支持 32 路多处理器

提示



由于 Windows Server 2003 Web 版只负责提供基本 Web 服务，所以对服务器硬件没有特殊要求，通常满足 Windows Server 2003 标准版需求的服务器即可。另外，对于某些 Intel Pentium Pro 或 Pentium II 处理器，Windows Server 2003 可能不使用多处理器，部署时应尤其注意。

1.2.2 安装方式

Windows Server 2003 操作系统可以利用多种方式安装，如使用光盘、硬盘及远程安装等。不同的安装方式适合于不同的环境，应根据实际情况选择。

1. 全新安装

利用 CD 启动计算机并运行安装程序安装是绝大部分服务都支持的方式，也是最基本的方法。新购买的服务器或者第 1 次部署网络服务器时，大多使用该方法。利用 Windows Server 2003 安装光盘可以直接启动服务器并安装，不需借助其他工具。不过，全新安装或者重新安装服务器时，往往需要使用服务器厂商提供的引导光盘或工具盘引导自动安装硬件设备所需的驱动程序。

2. 升级安装

如果计算机中已安装有 Windows NT Server 或 Windows 2000 Server 等操作系统，则不必卸载原来的 Windows 系统即可直接升级成 Windows Server 2003，而且升级后还可保留原来的配置。

从不同版本的 Windows Servers 产品升级到 Windows Server 2003 时，必须遵循表 1-2 中的升级原则。

表 1-2 升级原则

当前系统版本	可以升级到的 2003 版本	可以升级到的 R2 版本
Windows NT 4.0 Server	Windows Server 2003 标准版	Windows Server 2003 R2 标准版
Windows NT 4.0 Terminal Server		
Windows NT 4.0 Enterprise Edition		
Windows 2000 Server		
Windows 2000 Advanced Server	Windows Server 2003 企业版	Windows Server 2003 R2 企业版
Windows Server 2003 标准版		
Windows 2000 Server 数据中心版	Windows Server 2003 数据中心版	Windows Server 2003 R2 数据中心版

提示



- (1) Windows Server 2003 R2 中不包括 Web 版。
- (2) 经过本地化的产品不能跨越不同语言升级。
- (3) 支持 MUI 的 Windows Server 产品可以通过英文版升级。
- (4) 如果希望升级 Windows NT 4.0，则必须安装 Service Pack 5 (SP5) 或者更高版本的服务包。
- (5) 所有的 Windows 客户端操作系统均不能升级到 Windows Server 2003。
- (6) Windows Server 2003 R2 和 Windows Server 2003 SP2 是完全不同的两个概念，升级到 R2 时不必考虑其 SP 补丁的版本，也可在升级完成后安装 SP1 或 SP2。

3. 命令行安装

如果安装程序已复制到服务器硬盘中，可以直接将服务器启动到 DOS 模式下。然后运行安装目录中的 \i386\winnt.exe 的文件即可安装 Windows Server 2003 操作系统，并且在安装过程中不需要安装光盘。

4. 通过 Windows 部署服务远程安装

如果网络中已经部署了 Windows 部署服务器，而且服务器具有 PXE（预启动执行环境）功能，就可以通过网络远程安装 Windows Server 2003，还可以利用事先创建的自动应答文件实现无人值守安装。安装过程非常简单，只需在启动过程中根据提示信息按下引导键即可（一般为 F12 键），如图 1-3 所示。不过，采取这种安装方式必须确保计算机网卡支持 PXE，这是一种允许客户端从网络适配器开始启动序列的远程启动技术。如果网卡没有 PXE 引导芯片，则需要使用 `rbfg.exe` 程序生成启动软盘来远程安装。

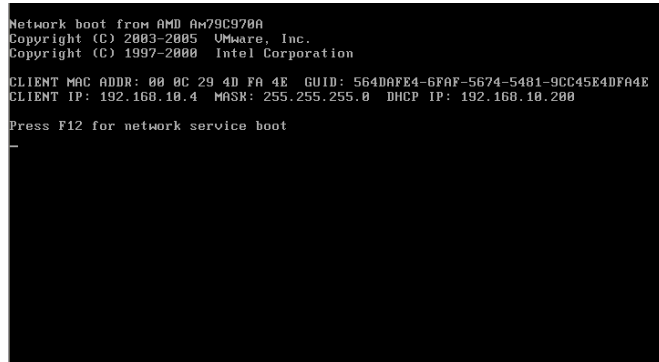


图 1-3 远程安装

1.2.3 安装前注意事项

为了保证 Windows Server 2003 系统能够顺利安装，在安装之前应当做好如下准备工作。

(1) 检查系统日志寻找错误

如果在计算机中安装有 Windows 2000/XP 系统，建议使用“事件查看器”查看系统日志，寻找可能在升级期间引发问题的最新错误或重复发生的错误。

(2) 检查硬件和软件兼容性

如果要从 Windows NT/2000 系统升级到 Windows Server 2003，为了保证服务器软件及硬件与 Windows Server 2003 兼容，避免出现兼容性故障，应在升级过程中运行兼容性检查向导检查是否有兼容性问题，以确定升级前是否需要更新硬件、驱动程序或软件。虽然有时即使出现兼容性问题也能继续升级，但可能会造成某些程序不能使用。另外，也可以通过访问网址“<http://www.microsoft.com/windows/catalog/>”检查 Windows Catalog 中的硬件和软件兼容性信息，确认是否兼容。

(3) 备份文件

如果服务器中已安装 Windows NT 等系统，为了避免安装后丢失重要数据，建议在升级前备份当前的文件，包括含有配置信息（例如，系统状态、系统分区和启动分区）的所有内容，以及所有的用户和相关数据。建议将文件备份到多种不同的媒体，例如，磁带驱动器或网络上其他计算机的硬盘，而尽量不要保存在本地计算机的其他非系统分区中。

(4) 切断硬件设备的连接

如果计算机正在与打印机、扫描仪及不间断电源（UPS）卡等非必要的外设连接，那么应在运行安装程序之前将其断开，避免安装程序在自动检测这类设备时出现问题。

(5) 断开网络

由于网络中可能会有病毒，如果未通过网络安装操作系统，那么在安装之前就应拔下网线，以免新安装的系统被感染上病毒。

(6) 加载驱动程序

由于服务器中往往安装有 RAID 卡等设备，而这些设备可能无法被 Windows 系统所识别，因此必须在安装之前加载相应的驱动程序。大多数品牌服务器出厂时就已经配备了引导光盘，用来加载驱动

程序并引导安装 Windows Server 2003。因此建议使用引导光盘安装。如果没有引导光盘，那么安装操作系统之前可以只加载 RAID 控制器的驱动程序；否则无法安装操作系统。至于其他设备的驱动程序，可以在系统安装完成后安装。

1.2.4 安装 Windows Server 2003、SP 和 R2

当准备工作做好以后，即可安装 Windows Server 2003。为了保护服务器的安全性和稳定性，还应当在操作系统安装完成后安装系统补丁（SP）及增加包（R2），它们可以从微软官方网站免费下载。

1. 安装 Windows Server 2003

① 将服务器 BIOS 设置为从光盘启动，并使用服务器引导光盘启动计算机，进入引导界面。图 1-4 所示是 DELL 服务器的引导画面，首先需要根据提示信息选择操作系统类型及版本等信息。

提示 如果不使用服务器引导光盘，而是直接使用 Windows Server 2003 安装光盘启动安装，就会直接启动到安装界面。如果硬盘内已安装有其他操作系统，则显示“Press any key to boot from CD.....”提示信息，如图 1-5 所示。此时按任意键，即可从光盘启动。



图 1-4 光盘引导界面

Press any key to boot from CD..._

图 1-5 提示信息

② 当驱动程序加载以后，即可从安装光盘启动，安装程序会检测计算机中的硬件设备。如果安装 Windows Server 2003 不支持的 RAID 卡或 SCSI 存储设备，则当安装程序界面底部显示“Press F6 if you need to install a third party SCSI or RAID driver...”提示信息时（如图 1-6 所示）必须按下 F6 键，准备为该 RAID 卡或 SCSI 设备提供驱动程序。

③ 安装程序提示将准备好的 SCSI 驱动程序软盘插入软驱，按 S 键开始安装，界面如图 1-7 所示。

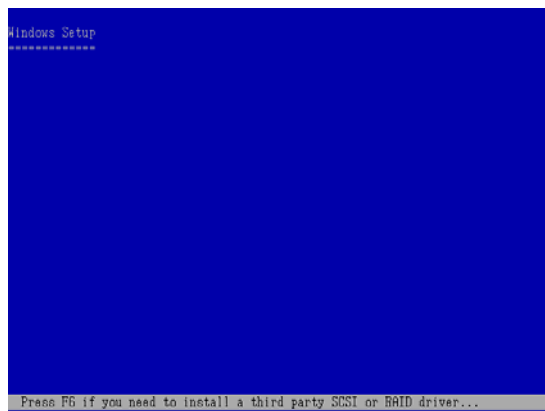


图 1-6 提示信息

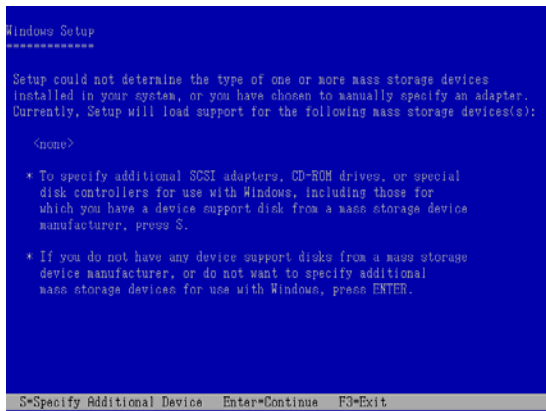


图 1-7 安装 SCSI 设备界面

- ④ 安装 SCSI 设备后按回车键,显示如图 1-8 所示界面,此时即可开始安装 Windows Server 2003。
- ⑤ 按回车键,显示如图 1-9 所示的 Windows 授权协议界面,要求阅读并接受微软 Windows Server 2003 许可协议。



图 1-8 开始安装 Windows Server 2003

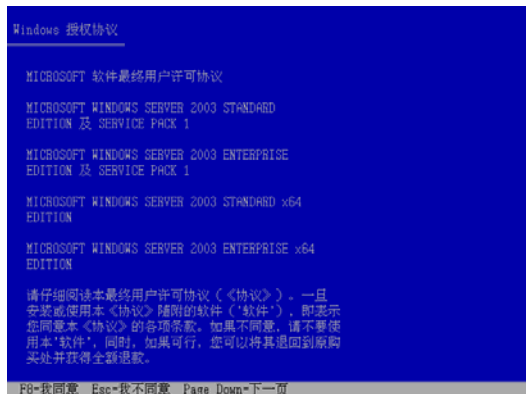


图 1-9 Windows 授权协议界面

- ⑥ 按 F8 键接受协议,显示如图 1-10 所示界面,提示需要为尚未分区的硬盘创建分区。
- ⑦ 按 C 键,显示如图 1-11 所示界面。在“创建磁盘分区大小”框中输入待划分的分区大小,创建第 1 个分区作为系统分区。为了便于维护和系统升级,建议将系统分区设置为 40 GB 或更多。按回车键,完成分区并返回,选择“未划分的空间”并划分为新分区。

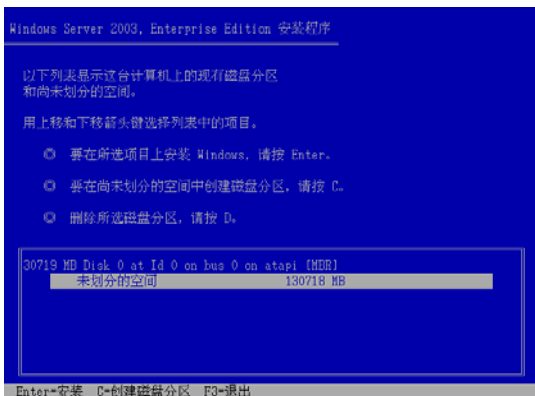


图 1-10 提示为尚未分区的硬盘分区

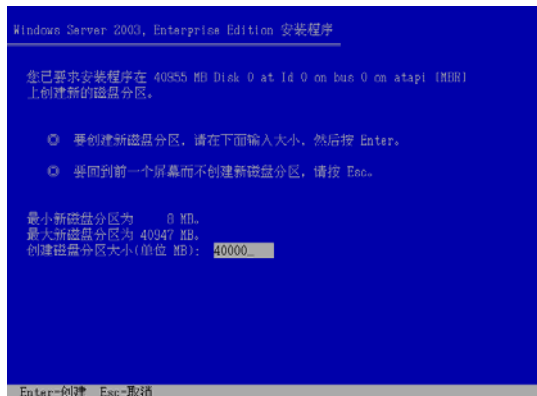


图 1-11 指定 C 盘磁盘空间

提示 创建系统分区完成后继续按下↑或↓箭头键移动到剩余空间创建其他分区,这些分区的格式化操作可以在安装完成后的“计算机管理”→“磁盘管理”中完成。另外,若分区设置错误,则按 D 键后按 L 键删除,然后重新创建分区。

- ⑧ 分区完成以后,选择 C 分区并按回车键。显示如图 1-12 所示的界面,选择“用 NTFS 文件系统格式化磁盘分区”选项。
- ⑨ 按回车键,开始格式化硬盘并向其中复制安装文件,完成后将自动重新启动。
- ⑩ 重新启动后,系统会自动检测计算机硬件配置。检测完成后显示如图 1-13 所示的“区域和语言选项”对话框,保留默认值即可。
- ⑪ 单击“下一步”按钮,显示如图 1-14 所示的“自定义软件”对话框,分别在“姓名”和“单位”文本框中输入用户姓名和单位名称。
- ⑫ 单击“下一步”按钮,显示如图 1-15 所示的“您的产品密钥”对话框。在“产品密钥”文本框中输入 Windows Server 2003 R2 的安装密钥。该密钥通常贴在包装袋封面上的黄色不干胶纸上,是一串分为 5 组,每组 5 位的数字。



图 1-12 选择“用 NTFS 文件系统格式化磁盘分区”选项

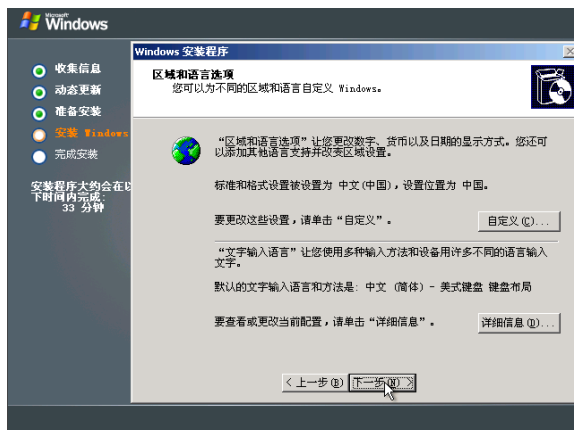


图 1-13 “区域和语言选项”对话框



图 1-14 “自定义软件”对话框

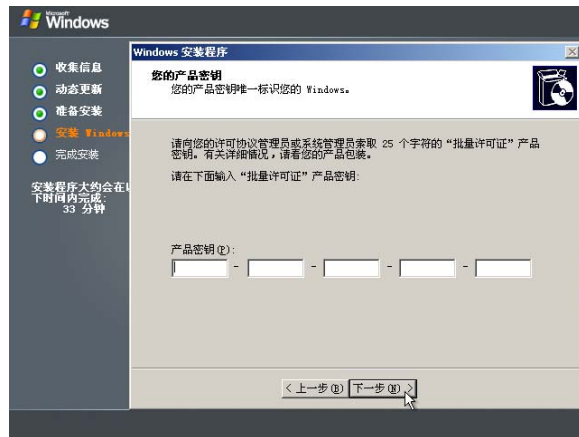


图 1-15 “您的产品密钥”对话框

⑬ 单击“下一步”按钮，显示如图 1-16 所示的“授权模式”对话框，选择授权方式及同时连接数。

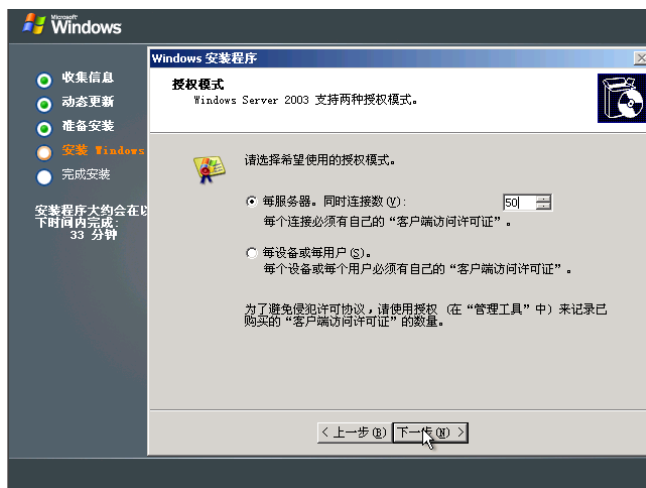


图 1-16 “授权模式”对话框

每服务器：每一个访问服务器的并发连接都需要有一个 CAL（Client Access License，客户访问许可证），为此要求每一台服务器在特定时刻都支持固定数量的连接。如果网络中的用户并不总是连接到该服务器，即可选择该模式指定该服务器允许的同时连接数，该数量由许可协议

规定。

每客户：每个访问 Windows 服务器的客户端计算机也需要有各自的 CAL，利用这个 CAL，客户计算机可以连接到任何数量的服务器。如果网络内有多台服务器运行，则可采用“每客户”许可证模式。



注意：

可以将许可证模式从“每服务器”转换为“每客户”，但是不能从“每客户”转换为“每服务器”。如果没有把握选择采用哪种许可证模式，建议选择“每服务器”模式，因为拥有一次免费从“每服务器”转换为“每客户”的机会。



⑭ 单击“下一步”按钮，显示如图 1-17 所示的“计算机名称和管理员密码”对话框。在“计算机名称”文本框中输入计算机名，在“管理员密码”及“确认密码”文本框中设置管理员密码。

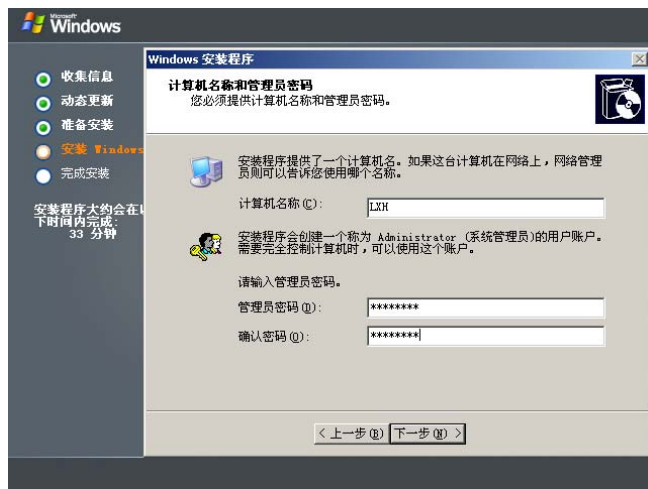


图 1-17 “计算机名称和管理员密码”对话框



提示

计算机名既要在网络中独一无二，又要能标识该服务器的身份。另外，必须牢记在这里输入的管理员密码；否则将无法登录系统。

⑮ 单击“下一步”按钮，显示如图 1-18 所示的“日期和时间设置”对话框，保留默认值即可。

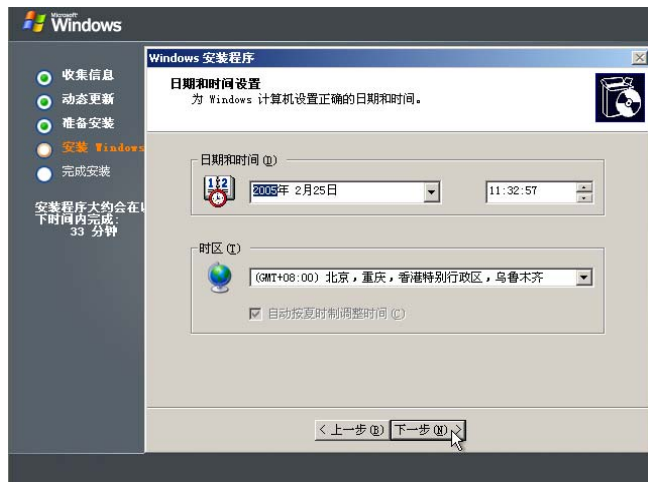


图 1-18 “日期和时间设置”对话框

①6 单击“下一步”按钮，显示如图 1-19 所示的“网络设置”对话框。选择“典型设置”单选按钮即可。如果需要现在设置 IP 地址及安装网络协议等，可选择“自定义设置”单选按钮。

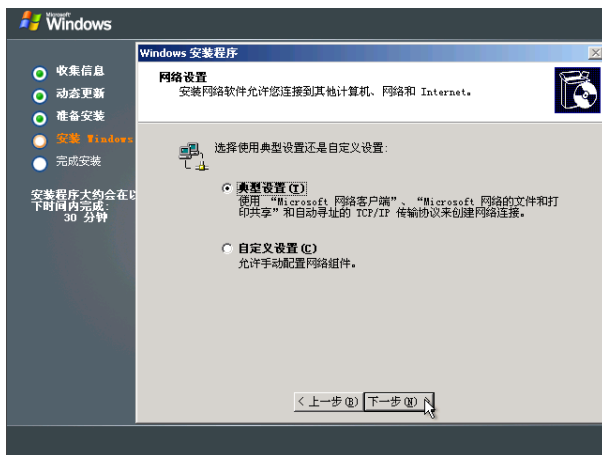


图 1-19 “网络设置”对话框

①7 单击“下一步”按钮，显示如图 1-20 所示的“工作组或计算机域”对话框，保留系统默认值即可。

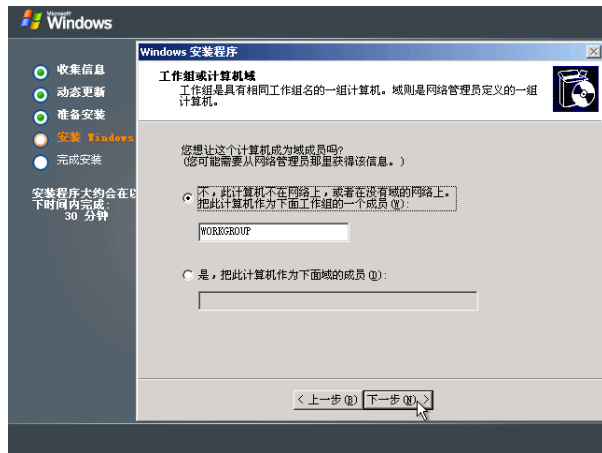


图 1-20 “工作组或计算机域”对话框

①8 单击“下一步”按钮，开始复制文件并安装系统。安装完成后自动重新启动，显示如图 1-21 所示的“欢迎使用 Windows”对话框。



图 1-21 “欢迎使用 Windows”对话框

19 按下 Ctrl + Alt + Delete 组合键，显示如图 1-22 所示的“登录到 Windows”对话框，在“密码”文本框中输入安装时设置的管理员密码。

20 单击“确定”按钮登录系统，默认启动“管理您的服务器”窗口，如图 1-23 所示。



图 1-22 “登录到 Windows”对话框

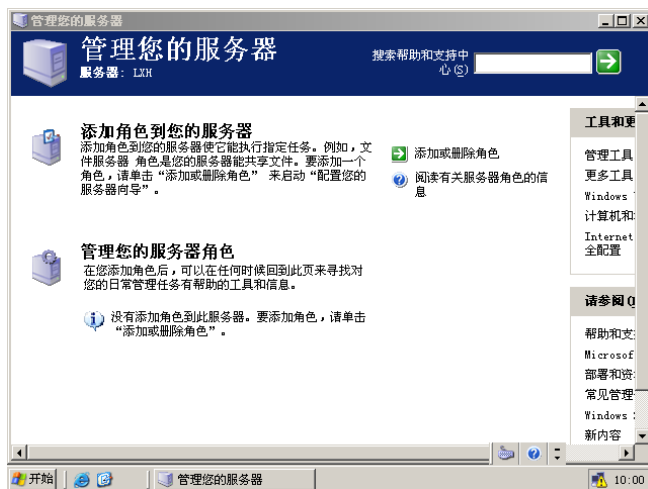


图 1-23 “管理您的服务器”窗口

2. 安装 SP 和 R2

为了保护 Windows 系统的安全性和稳定性并提高系统性能，微软公司会经常在其网站发布一些 Windows 系统补丁程序，如 SP1 和 SP2 等，以及一些系统增强包 R2。由于 R2 和 SP1 和 SP2 的安装方式相同，并且 R2 中已经集成了 SP1，因此这里只介绍 R2 的安装。

1 将 Windows Server 2003 R2 安装光盘放入光驱，或者运行已下载的 R2 安装程序。显示“Windows Server 2003 R2 安装程序向导”对话框，如图 1-24 所示。

2 单击“下一步”按钮，显示如图 1-25 所示的“最终用户许可协议”对话框，选择“我接受许可协议中的条款”单选按钮。



图 1-24 “Windows Server 2003 R2 安装程序向导”对话框



图 1-25 “最终用户许可协议”对话框

3 单击“下一步”按钮，复制文件并安装。安装完成后，显示如图 1-26 所示的“正在完成 Windows Server 2003 R2 安装程序”对话框。

4 单击“完成”按钮退出安装向导，显示如图 1-27 所示的“Windows Server 后安装安全更新”窗口。在其中可以配置服务器更新，以保护系统安全。

5 单击“完成”按钮关闭窗口，Windows Server 2003 R2 安装完成。



图 1-26 “正在完成 Windows Server 2003 R2 安装程序”对话框

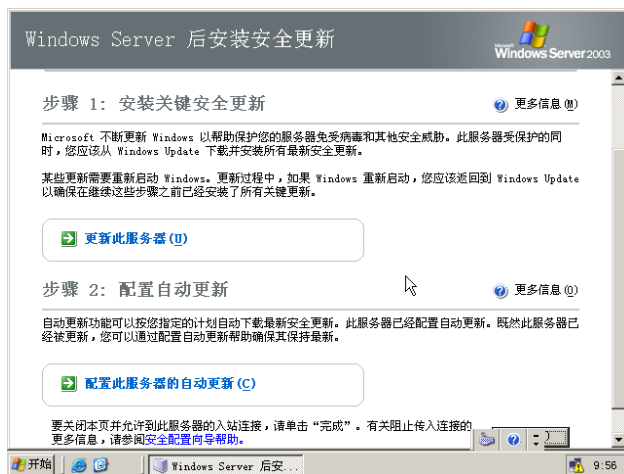


图 1-27 “Windows Server 后安装安全更新”窗口

1.2.5 升级 Windows Server 2003

如果服务器中原来安装的是 Windows NT 或者 Windows 2000 Server 系统，而且保存了许多重要数据，则可利用升级功能直接升级到 Windows Server 2003，以保留原来的数据。

1. 检查系统兼容性

① 登录到 Windows 2000 Server 系统，将 Windows Server 2003 安装光盘放入光驱并自动运行，显示如图 1-28 所示的“欢迎使用 Windows Server 2003”界面。

② 单击“检查系统兼容性”超级链接，显示如图 1-29 所示的“您希望做什么”界面。



图 1-28 “欢迎使用 Windows Server 2003 家族”界面



图 1-29 “您希望做什么”界面

③ 单击“自动检查我的系统”超级链接，显示如图 1-30 所示的“获得更新的安装程序文件”对话框，用来从微软网站获得更新的安装程序文件。如果不想获得更新文件，可选择“否，跳过这一步继续安装 Windows”单选按钮。

④ 单击“下一步”按钮开始检查系统配置，完成后显示如图 1-31 所示的“报告系统兼容性”对话框。其中列出所有与 Windows 不兼容的项目，在安装过程中或安装完成后，这些项目可能无法使用。单击“详细信息”按钮可以查看各个项目的详细情况；单击“另存为”按钮可以将当前信息保存为报告文件。

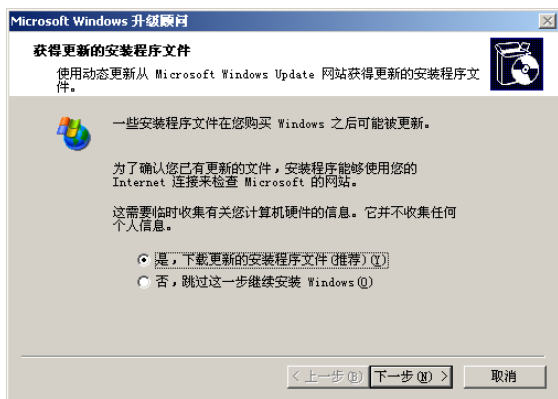


图 1-30 “获得更新的安装程序文件”对话框

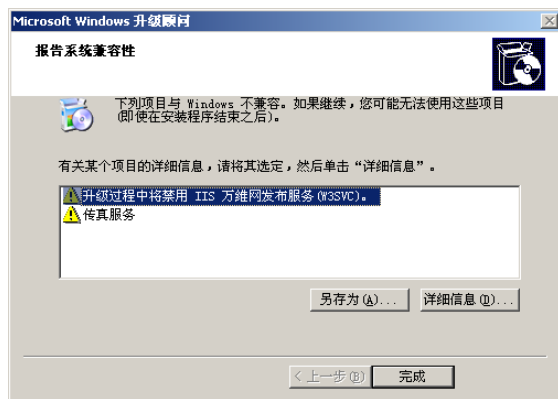


图 1-31 “报告系统兼容性”对话框

⑤ 单击“完成”按钮，兼容性检查完成。如果检查结果对安装无影响，则可安装 Windows Server 2003。

2. 升级 Windows Server 2003

① 运行 Windows Server 2003 安装光盘，在“欢迎使用 Windows Server 2003”界面中单击“安装 Windows Server 2003”超级链接，显示如图 1-32 所示的“欢迎使用 Windows 安装程序”对话框，在“安装类型”下拉列表框中选择“升级（推荐）”选项。

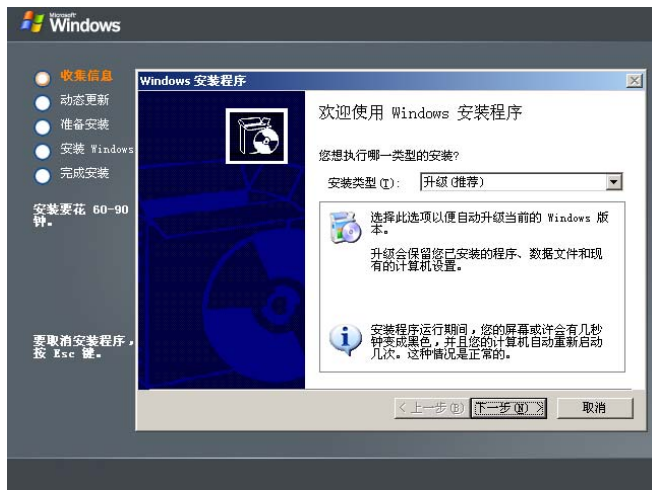


图 1-32 “欢迎使用 Windows 安装程序”对话框

② 单击“下一步”按钮，显示如图 1-33 所示的“许可协议”对话框，选择“我接受这个协议”单选按钮。

③ 单击“下一步”按钮，显示如图 1-34 所示的“您的产品密钥”对话框，输入 Windows Server 2003 安装序列号。



图 1-33 “许可协议”对话框

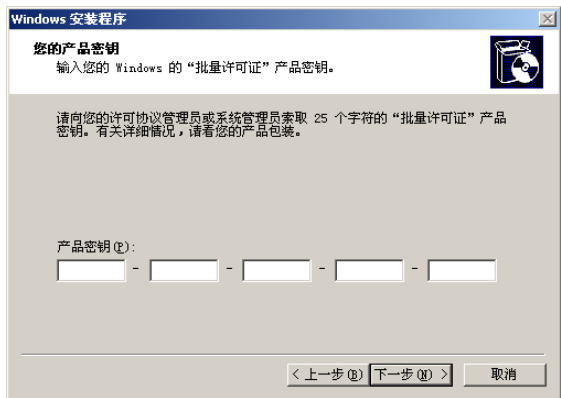


图 1-34 “您的产品密钥”对话框

④ 单击“下一步”按钮，显示如图 1-35 所示的“获得更新的安装程序文件”对话框，建议选择“否，跳过这一步继续安装 Windows”单选按钮。

⑤ 单击“下一步”按钮，安装向导开始复制文件，完成后会自动重新启动计算机。显示如图 1-36 所示的启动菜单，默认状态下 5 秒钟后将自动开始 Windows Server 2003 安装程序。

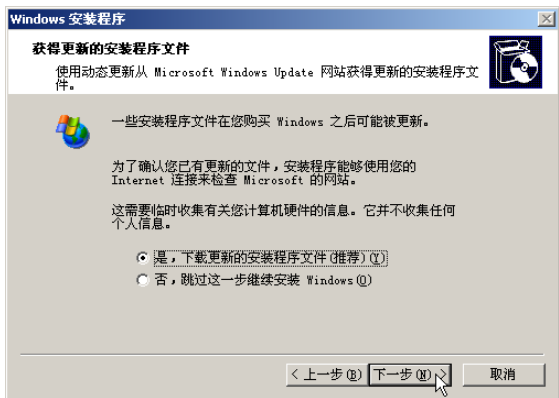


图 1-35 “获得更新的安装程序文件”对话框

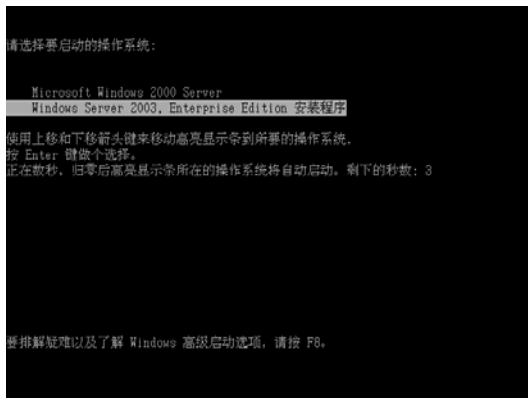


图 1-36 启动菜单

⑥ 启动以后显示如图 1-37 所示的界面，准备安装并删除 Windows 2000 Server 的部分系统文件。



图 1-37 准备安装 Windows Server 2003

后续的操作与直接安装 Windows Server 2003 相同，这里不复赘述。

安装完成之后即可登录 Windows Server 2003 系统，而原有 Windows 2000 Server 部分系统配置仍然保留。

1.2.6 添加与管理网络服务

Windows Server 2003 自带了多种网络服务,用来为网络提供各种功能。添加网络服务可以借助“配置您的服务器向导”和“Windows 组件向导”两种方式,完成后可以利用服务自带的控制台管理。

1. 添加网络服务

“配置您的服务器向导”是添加或删除 Windows 服务的常用方法之一,也是 Windows Server 2003 系统中的新增功能,操作步骤如下。

- ① 登录到 Windows Server 2003 系统,自动打开如图 1-38 所示的“管理您的服务器”窗口。

提示 也可单击“开始”→“管理您的服务器”选项,或者单击“开始”→“管理工具”→“管理您的服务器”选项打开“管理您的服务器”窗口。



- ② 单击“添加或删除角色”超级链接,显示如图 1-39 所示的“预备步骤”对话框,提示在安装网络服务之前应当做好的准备工作。

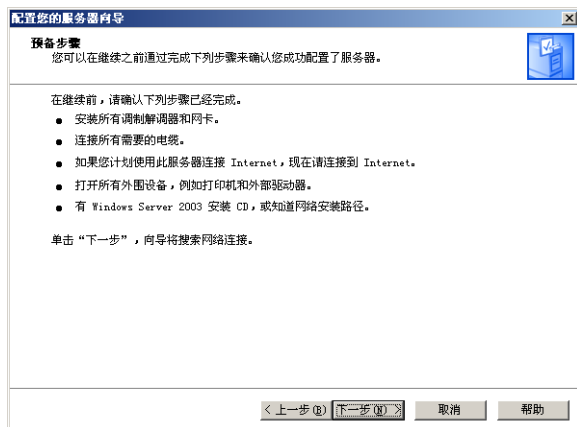


图 1-39 “预备步骤”对话框

- ③ 单击“下一步”按钮,系统开始检查网络连接设置,如图 1-40 所示。
- ④ 检查完毕后,显示如图 1-41 所示的“配置选项”对话框。如果该服务器是网络中的第 1 台服务器,并准备将其配置为域控制器、DHCP 服务器和 DNS 服务器,则选择“第一台服务器的典型配置”单选按钮;如果只是安装某种服务,则选择“自定义配置”单选按钮。

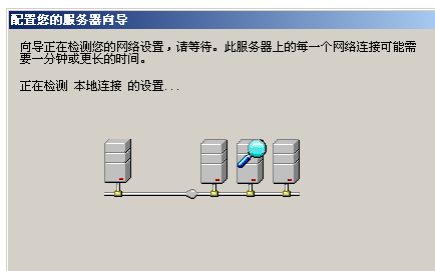


图 1-40 检查网络连接设置

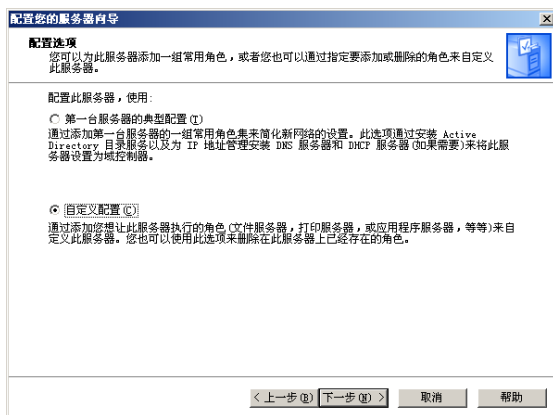


图 1-41 “配置选项”对话框

⑤ 单击“下一步”按钮，显示如图 1-42 所示的“服务器角色”对话框。所有可安装的网络服务全部显示在列表框中，可以选择待安装的网络服务。如果“已配置”列中显示为“否”，说明该网络服务尚未安装；显示为“是”，说明该网络服务已经安装。

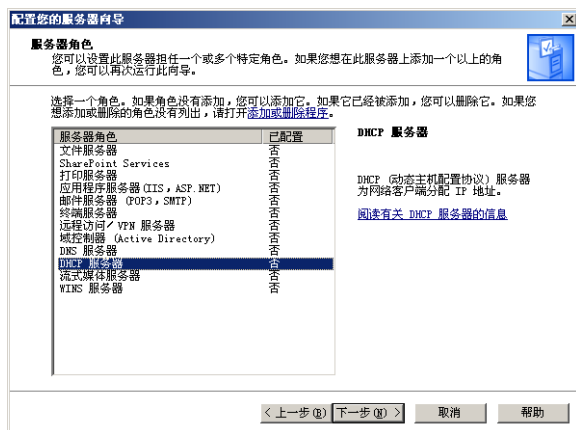


图 1-42 “服务器角色”对话框

⑥ 单击“下一步”按钮开始安装，并根据系统提示插入系统安装盘即可。安装完成以后，所有安装的服务都会显示在“管理您的服务器”窗口中，如图 1-43 所示。有些网络服务可能会在安装过程中调用配置向导做一些简单的配置，但更详细的配置通常需借助于安装完成后的网络管理实现。



图 1-43 已安装的服务

如果需要删除有些服务，可再次运行“配置您的服务器向导”。在“服务器角色”对话框中选择已安装的服务，并单击“下一步”按钮，显示如图 1-44 所示的“角色删除确认”对话框。选中“删除 XXX 服务器角色”复选框，单击“下一步”按钮即可将其删除。

如果有些服务无法通过“配置您的服务器向导”安装，或者需要同时安装多个服务，则可以利用如图 1-45 所示的“Windows 组件向导”安装。选中相应组件的复选框，单击“下一步”按钮，并根据系统提示插入 Windows Server 2003 安装光盘即可。如果要卸载某个组件，可清除相应的复选框。

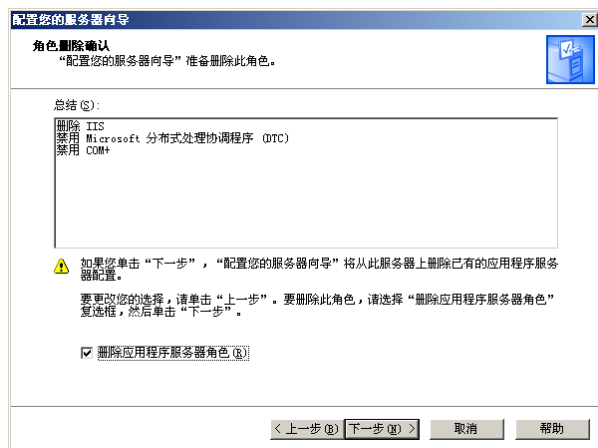


图 1-44 “角色删除确认”对话框



图 1-45 “Windows 组件向导”对话框

2. 管理网络服务

安装完成网络服务以后，通常会启动并向网络提供相应的服务。但是有些服务需要重新配置，此时可以在“管理您的服务器”窗口中打开相应的服务，也可以通过“开始”菜单打开。

在“管理您的服务器”窗口中单击待管理的服务右侧的“管理此 XXX 服务器角色”，打开管理该服务的窗口，如图 1-46 所示，可以配置管理该服务。

另外，也可以单击“开始”→“管理工具”选项，然后单击待管理的服务名称，打开相应的服务控制台。

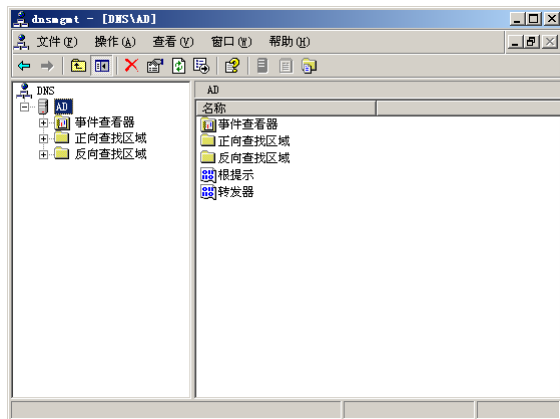


图 1-46 管理服务窗口

1.2.7 Windows Server 2003 控制台

Microsoft 管理控制台 (Microsoft Management Console, MMC) 是 Windows Server 2003 中内置的一个组件，版本为 3.0。它可以用来管理本地或远程计算机 Windows 系统中的一些服务，并可以同时管理多个服务。不过管理服务之前，需要首先添加相应的管理插件。

① 单击“开始”→“运行”选项，显示如图 1-47 所示的“运行”对话框。

② 在“运行”文本框中输入“mmc”命令，单击“确定”按钮打开 MMC 管理控制台，如图 1-48 所示。

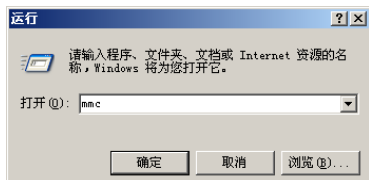


图 1-47 “运行”对话框

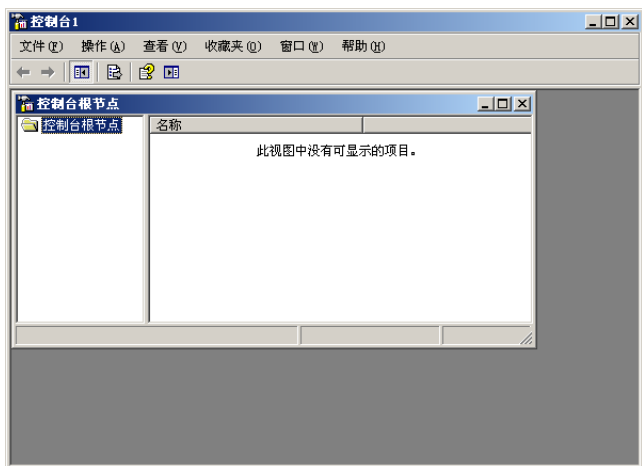


图 1-48 MMC 管理控制台

③ 单击“文件”→“添加/删除管理单元”选项，显示“添加/删除管理单元”对话框，如图 1-49 所示。

④ 单击“添加”按钮，显示如图 1-50 所示的“添加独立管理单元”对话框，其中列出当前计算机中安装的所有 MMC 插件。



图 1-49 “添加/删除管理单元”对话框



图 1-50 “添加独立管理单元”对话框

⑤ 选择要添加的组件，单击“添加”按钮。如果添加的插件也可以管理远程计算机，则显示一个对话框。选择“本地计算机”单选按钮用来管理当前计算机；选择“另一台计算机”单选按钮并输入另一台计算机的名称或 IP 地址，则可用来管理远程计算机，如图 1-51 所示。

⑥ 单击“完成”按钮，然后先后单击“关闭”及“确定”按钮。所选管理单元显示在控制台中，如图 1-52 所示，可添加多个管理单元。此时，即可在 MMC 控制台中管理所需服务。

⑦ 为了方便以后再次打开这些管理单元，可单击“控制台”→“保存”选项，将控制台保存为文件。



注意： 在使用 MMC 管理网络上其他计算机中的服务时，必须拥有待管理计算机的相应权限，并且在本地计算机上安装有相应的 MMC 插件。



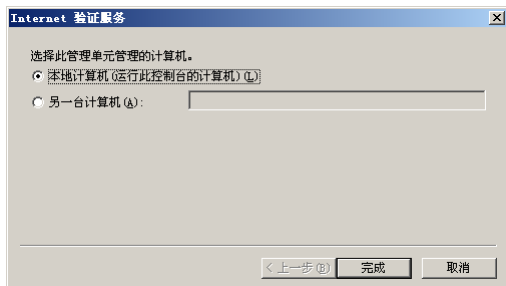


图 1-51 选择管理的计算机

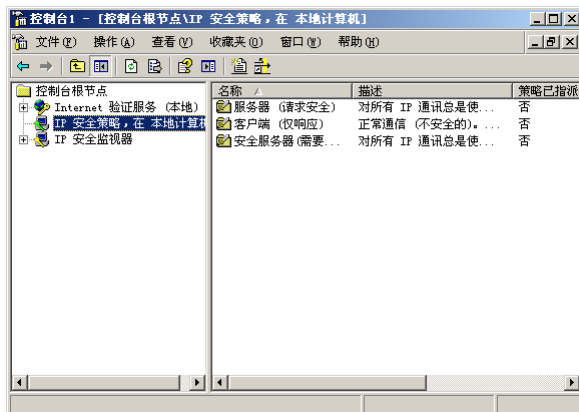


图 1-52 添加插件后的控制台

1.2.8 Windows Server 2003 系统设置

安装 Windows Server 2003 以后，还需要安装硬件设备驱动程序、格式化分区、设置 IP 地址信息，以及设置用户账户密码等。

1. 安装驱动程序

根据网络需要不同，服务器可能增加一些硬件设备。而在服务器随机附带的引导光盘中可能并没有相应的驱动程序，因此需要在操作系统安装完成以后手动安装硬件设备的驱动程序。

① 单击“开始”→“管理工具”→“计算机管理”选项，打开“计算机管理”窗口，如图 1-53 所示。

② 在左窗格中单击“设备管理器”选项，在右窗格的“其他设备”中即可看到没有安装驱动程序的设备。通常显示为黄色的问号或感叹号，如图 1-54 所示。

③ 通常计算机中的各硬件设备都带有各自的驱动程序光盘，只需运行其中的安装程序并根据提示重新启动计算机即可。安装完成后，即可正确显示各硬件设备的型号等信息，如图 1-55 所示。

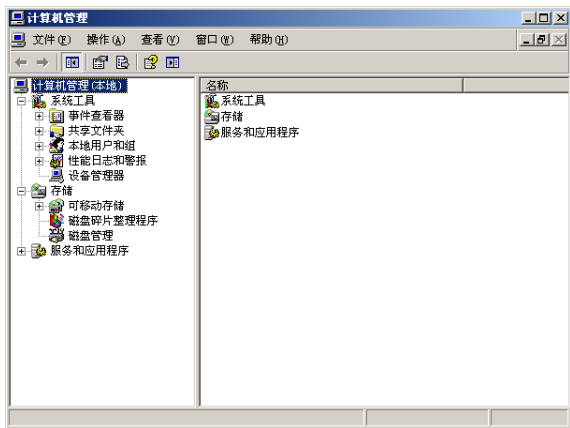


图 1-53 “计算机管理”窗口

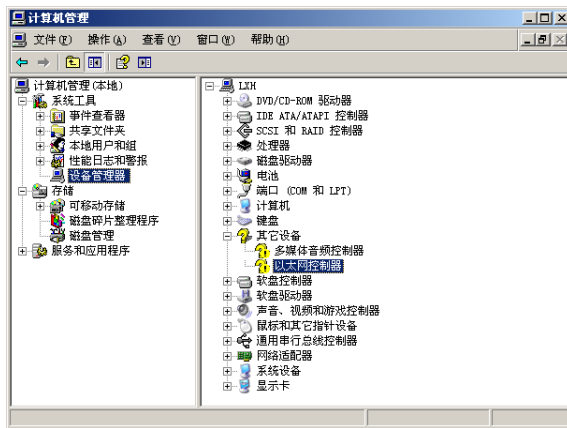


图 1-54 黄色的问号或感叹号表示未安装驱动程序的设备

2. 格式化分区

Windows Server 2003 在安装过程中可以为硬盘分区，但只能格式化系统分区，因此需要在安装完成后格式化其他分区。

① 打开“我的电脑”窗口，选择尚未格式化的分区。右击并选择快捷菜单中的“格式化”选项，显示如图 1-56 所示的“格式化”对话框。在“文件系统”下拉列表框中选择待使用的分区格式，例如 NTFS。为了加快格式化速度，可选中“快速格式化”复选框。

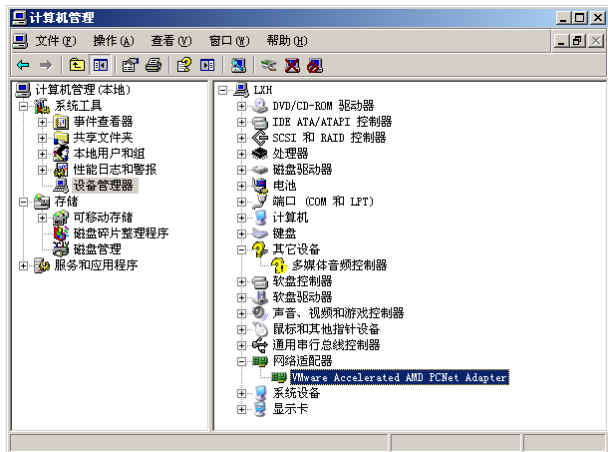


图 1-55 安装完成驱动程序显示的信息

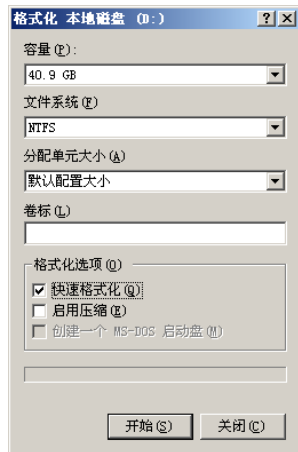


图 1-56 “格式化”对话框

提示 双击打开尚未格式化的分区时，显示如图 1-57 所示的“磁盘未格式化”提示框。提示磁盘没有格式化，单击“是”按钮即可打开“格式化”对话框。

- ② 单击“开始”按钮，显示如图 1-58 所示的警告框，提示格式化将删除该盘中的数据。

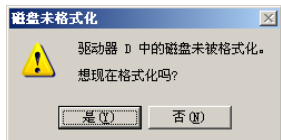


图 1-57 “磁盘未格式化”提示框

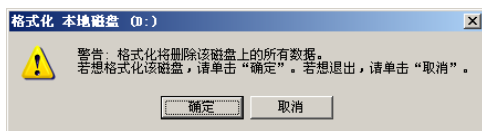


图 1-58 警告框

- ③ 单击“确定”按钮，即可开始格式化。完成后显示如图 1-59 所示的提示框，提示格式化完成。

- ④ 单击“确定”按钮格式化完成，单击“关闭”按钮关闭。

按照同样步骤，可以继续格式化其他尚未格式化的分区。

3. 设置 IP 地址

如果网络中部署有 DHCP 服务器，那么计算机可以自动获取 IP 地址；否则需要手动设置固定的 IP 地址信息。通常为了便于管理和访问，服务器通常都设置固定的 IP 地址。

- ① 单击“开始”→“控制面板”→“网络连接”→“本地连接”选项，显示如图 1-60 所示的“本地连接 状态”对话框。



图 1-59 提示框



图 1-60 “本地连接 状态”对话框

提示 也可以单击“开始”→“控制面板”选项，双击“网络连接”图标，显示如图 1-61 所示的“网络连接”窗口。本地计算机上的网卡显示为“本地连接”图标，右击该图标并选择快捷菜单中的“属性”选项打开“本地连接 属性”对话框。

② 单击“属性”按钮，显示如图 1-62 所示的“本地连接 属性”对话框。如果服务器中安装有多块网卡，应当分别选择并一一设置。

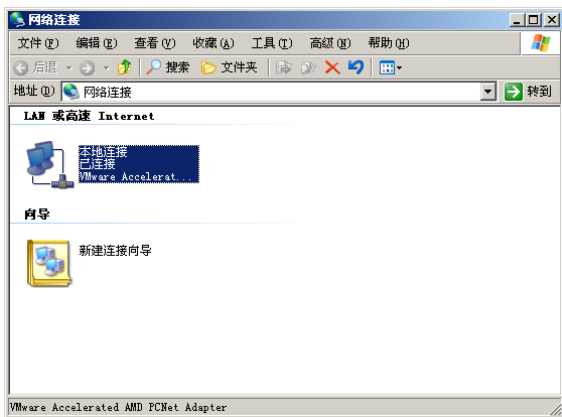


图 1-61 “网络连接”窗口

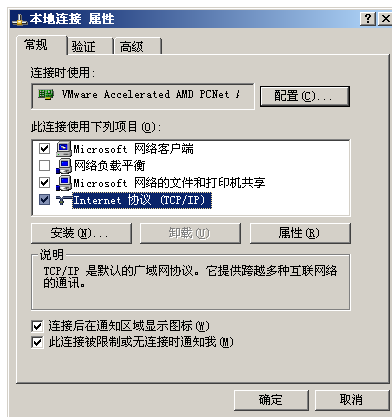


图 1-62 “本地连接 属性”对话框

③ 在“此连接使用下列项目”列表框中选择“Internet 协议 (TCP/IP)”选项，单击“属性”按钮，显示如图 1-63 所示的“Internet 协议 (TCP/IP) 属性”对话框。如果要从 DHCP 服务器自动获取 IP 地址，则保留选择默认的“自动获得 IP 地址”单选按钮。

④ 如果要手动配置 IP 地址，则选择“使用下面的 IP 地址”和“使用下面的 DNS 服务器地址”单选按钮。分别输入 IP 地址、子网掩码、默认网关、首选 DNS 服务器和备用 DNS 服务器，设置有关选项，如图 1-64 所示。

⑤ 如果需要为一块网卡指定多个 IP 地址或者网关，则单击“高级”按钮，显示“高级 TCP/IP 设置”对话框。在“IP 设置”选项卡的“IP 地址”文本框组中单击“添加”按钮可添加多个 IP 地址，如图 1-65 所示；单击“默认网关”选项组中的“添加”按钮，则可添加多个网关。

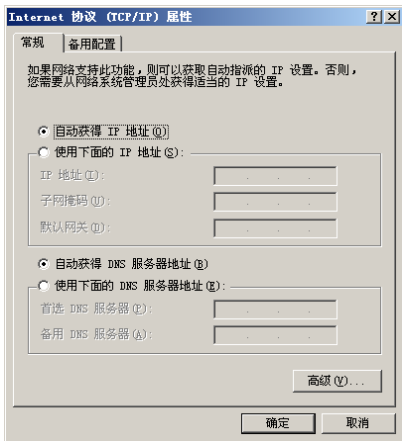


图 1-63 “Internet 协议 (TCP/IP) 属性”对话框

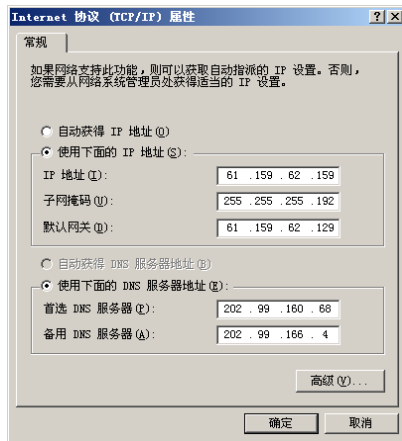


图 1-64 设置有关选项

⑥ 单击“确定”按钮保存设置，IP 地址设置完成。

4. 设置自动更新

为了使 Windows Server 2003 系统时刻保持在最安全状态，应当启动自动更新功能，以及及时从微软

网站下载最新补丁程序。

① 右击“我的电脑”图标，选择快捷菜单中的“属性”选项，打开“系统属性”对话框。打开“自动更新”选项卡（如图 1-66 所示），可以在其中选择自动更新的方式。



图 1-65 添加多个 IP 地址

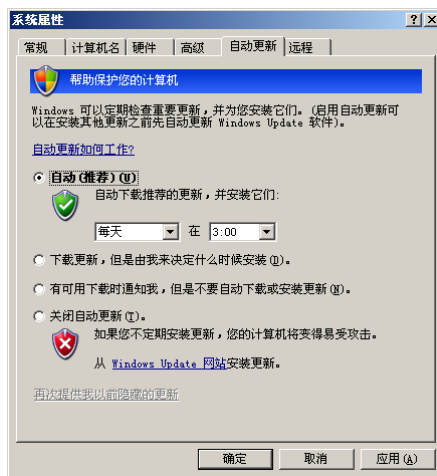


图 1-66 “自动更新”选项卡

“自动（推荐）”复选框：选择后系统定时下载并安装更新，通常设置在用户不使用网络的时间，以节省网络带宽。

“下载更新，但是由我来决定什么时候安装。”复选框：选择后系统自动检查并下载更新，并提示用户安装。

“有可用下载时通知我，但是不要自动下载或安装更新。”复选框：选择后系统发现有更新程序时不会自动下载，而是通知用户下载安装。

“关闭自动更新”复选框：选择后关闭自动更新功能。

② 单击“确定”按钮，系统将按照设置的选项更新。

1.3 安装 Windows Server 2008

Windows Server 2008 是迄今为止微软发布的最成熟的操作系统，无论是安全性、稳定性及功能等方面都有相当大的提高。其安装方式大大简化，安装过程中不需要设置计算机名及用户账户等信息，而且全程只需 10 多分钟，大大提高了工作效率。

1.3.1 系统和硬件设备要求

Windows Server 2008 对计算机的硬件配置要求较高，而且不同的版本对计算机硬件配置的要求也不一样，如表 1-3 所示。

表 1-3 不同版本的 Windows Server 2008 系统的需求

需 求	标准版	企业版	数据中心版	安腾版
CPU 最低速率	32 位：1 GHz 64 位：1.4 GHz	32 位：1 GHz 64 位：1.4 GHz	32 位：1 GHz 64 位：1.4 GHz	Itanium: Itanium 2
CPU 推荐速率	2 GHz 或更快	2 GHz 或更快	2 GHz 或更快	2 GHz 或更快
内存最小容量	512 MB	512 MB	1 GB	1 GB
内存推荐容量	2 GB	3 GB	2 GB	2 GB
内存最大容量	32 位：4 GB 64 位：32 GB	32 位：64 GB 64 位：2 TB	32 位：64 GB 64 位：2 TB	2 TB

续表

需 求	标准版	企业版	数据中心版	安腾版
支持的 CPU 个数	1~4	1~8	8~32	1~64
所需硬盘空间	最小 10 GB 推荐 40 GB 或更大	最小 10 GB 推荐 40 GB 或更大	最小 10 GB 推荐 40 GB 或更大	最小 10 GB 推荐 40 GB 或更大
群集节点数	无	最多 8 个	最多 8 个	

其他硬件配置，如显示设备、网络适配器、光驱软驱、键盘和鼠标等均要保证与 Windows Server 2008 相兼容。

提示 除安腾版之外的 Windows Server 2008 64 位系统都必须安装经过数字签名的核心模式驱动程序，否则会被拒绝或导致运行错误。要禁用数字签名驱动功能，可以在系统启动时按 F8 键。选择高级启动选项，然后选择禁用驱动签名检查即可。

注意 当服务器内存大于 16 GB 时，建议相应增加系统分区，以便存储页面文件或启用休眠功能。

1.3.2 安装方式

选择合适的安装方式可以减少很多不必要的麻烦，Windows Server 2008 有多种安装方式，分别适用于不同的环境。服务器操作系统毕竟不同于个人计算机系统，无论是从安全性，还是稳定性都是要仔细考虑的。

一般情况下，可以通过如下几种方法安装 Windows Server 2008 操作系统。

(1) 全新安装

使用 CD 启动计算机并安装，这是最基本的方法，也为绝大部分计算机所支持。全新安装或者重新安装服务器时，往往会用到服务器厂商提供的引导光盘或工具盘，然后根据提示信息适时插入 Windows Server 2008 安装光盘即可。

(2) 升级安装

如果计算机中原来安装的是 Windows Server 2003 等操作系统，则可以直接升级成 Windows Server 2008。并且不需要卸载原来的 Windows 系统，只要在原来的系统基础上进行升级安装即可，升级后还可保留原来的配置。

从不同版本的 Windows Server 2003 可以升级到不同版本的 Windows Server 2008，表 1-4 所示为不同版本操作系统的升级原则。

表 1-4 升级原则

当前系统版本	可以升级到的 2008 版本
Windows Server 2003 R2 标准版	Windows Server 2008 标准版
Windows Server 2003 标准版 (SP1)	Windows Server 2008 企业版
Windows Server 2003 标准版 (SP2)	
Windows Server 2003 R2 企业版	Windows Server 2008 企业版
Windows Server 2003 企业版 (SP1)	
Windows Server 2003 企业版 (SP2)	

(3) 通过 Windows 部署服务远程安装

和 Windows Server 2003 一样，Windows Server 2008 也支持通过网络从 Windows 部署服务安装。

并且可以通过应答文件实现自动安装，当然前提是服务器必须具有 PXE 功能。

(4) Server Core 安装

除 Windows Server 2008 安腾版以外，其他几个版本都支持 Server Core 安装，如图 1-67 所示。

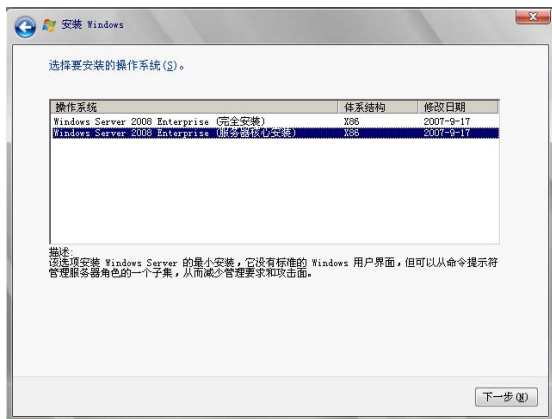


图 1-67 Server Core

1.3.3 安装前注意事项

为了保证 Windows Server 2008 的顺利安装，在开始安装之前也必须做好准备工作，包括检查日志错误、备份文件、断开网络并断开非必要的硬件连接等。所不同的是，Windows Server 2008 对硬盘空间要求比较大，系统分区至少为 10 GB。不过为了保证系统更好的运行，以及为安装其他软件做准备，应设置为 40 GB 或更大。

另外，由于 Windows Server 2008 安装程序比较大，采用 DVD 光盘，因此服务器必须配备 DVD 光驱。

1.3.4 安装 Windows Server 2008

安装 Windows Server 2008 的步骤如下。

① 使用 Windows Server 2008 安装光盘启动计算机，进入 Windows Server 2008 安装向导。首先显示“安装 Windows”对话框，如图 1-68 所示。默认安装语言为“中文（简体）”，时间和货币格式为“中文（简体），中国”，键盘和输入方法为“中文（简体）-美式键盘”，保留默认设置即可。

② 单击“下一步”按钮，提示准备安装，如图 1-69 所示。



图 1-68 Windows Server 2008 安装界面



图 1-69 准备安装

③ 单击“现在安装”按钮，显示如图 1-70 所示的“选择要安装的操作系统”对话框。在“操作系统”列表框中列出了可以安装的操作系统版本，这里选择“Windows Server 2008 Enterprise（完全安装）”选项，即安装 Windows Server 2008 企业版。

④ 单击“下一步”按钮，显示如图 1-71 所示的“请阅读许可条款”对话框。阅读许可条款，并且必须接受许可条款才可继续安装。

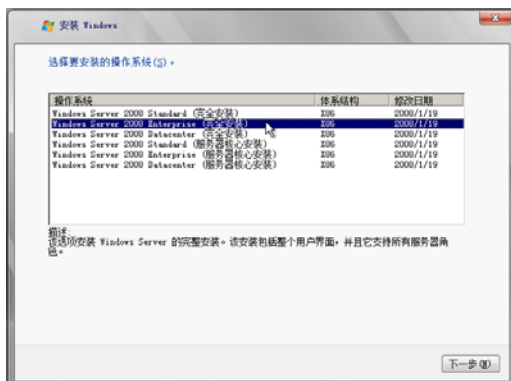


图 1-70 “选择要安装的系统”对话框



图 1-71 “请阅读许可条款”对话框

⑤ 选中“我接受许可条款”复选框，单击“下一步”按钮，显示如图 1-72 所示的“您想进行何种类型的安装？”对话框。其中，“升级”选项用于从 Windows Server 2003 升级到 Windows Server 2008，如果当前计算机没有安装操作系统，该选项不可用；而“自定义（高级）”选项则用于全新安装。

⑥ 单击“自定义（高级）”选项，显示如图 1-73 所示的“您想将 Windows 安装在何处？”对话框。其中显示当前计算机上硬盘的分区信息，这里提示该服务器中的硬盘尚未分区。



图 1-72 “您想进行何种类型的安装？”对话框



图 1-73 “您想将 Windows 安装在何处？”对话框

⑦ 单击“驱动器选项（高级）”链接，显示如图 1-74 所示的硬盘信息。在其中可以分区及格式化硬盘，并且删除硬盘的已有分区等。

⑧ 现在分区硬盘，单击“新建”按钮。在“大小”文本框中输入第 1 个分区的大小，例如 80 000 MB，如图 1-75 所示。



图 1-74 硬盘信息

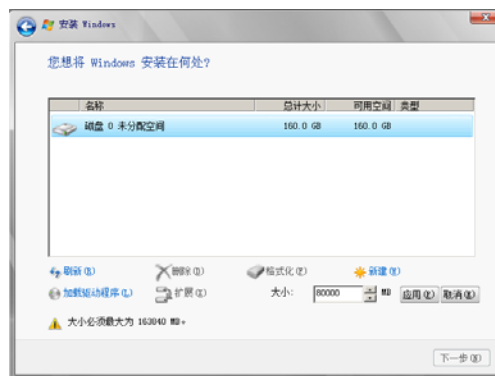


图 1-75 输入分区的大小

- ⑨ 单击“应用”按钮，第 1 个分区完成，如图 1-76 所示。
- ⑩ 选择“磁盘 0 未分配空间”选项，单击“新建”按钮将剩余空间划分为其他分区，如图 1-77 所示。按照此方法划分的全部分区默认为主分区。

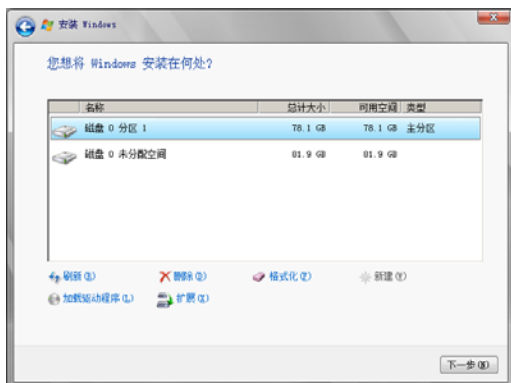


图 1-76 第 1 个分区完成



图 1-77 划分其他分区

- ⑪ 为选择第 1 个分区作为主分区用来安装操作系统，单击“下一步”按钮，显示如图 1-78 所示的“正在安装 Windows”对话框，开始复制文件并安装 Windows。
- ⑫ 在安装过程中，系统会根据需要自动重新启动。安装完成后，显示如图 1-79 所示的界面，提示第 1 次登录之前必须更改密码。



图 1-78 “正在安装 Windows”对话框

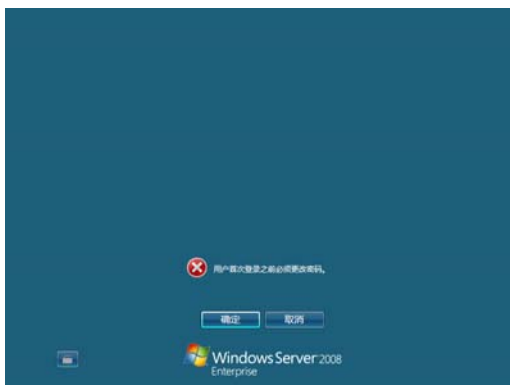


图 1-79 提示更改密码

- ⑬ 单击“确定”按钮，显示如图 1-80 所示的界面，提示设置密码。
- ⑭ 在“新密码”和“确认密码”文本框中输入密码，然后按回车键。密码更改成功，如图 1-81 所示。

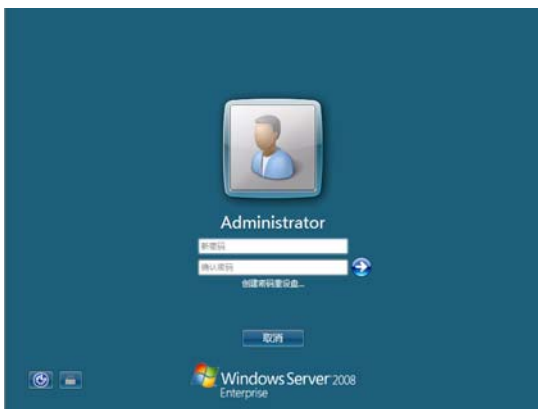


图 1-80 提示更改密码

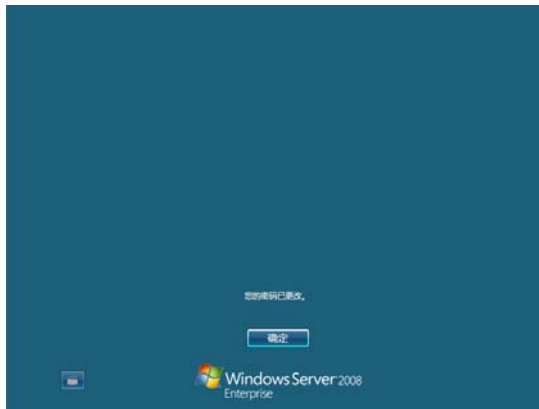


图 1-81 密码更改成功



注意：

和以往的操作系统不同，Windows Server 2003 系统仅建议使用强密码，但在非域环境中仍允许为用户账户设置简单密码；而在 Windows Server 2008 系统中必须设置强密码，否则将提示“无法更新密码。为新密码提供的值不符合字符域的长度、复杂性或历史要求”，如图 1-82 所示。



15 单击“确定”按钮，显示如图 1-83 所示的登录界面，需要用刚刚设置的密码登录系统。

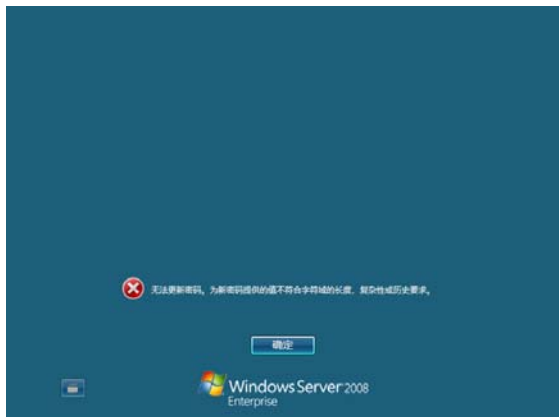


图 1-82 提示信息

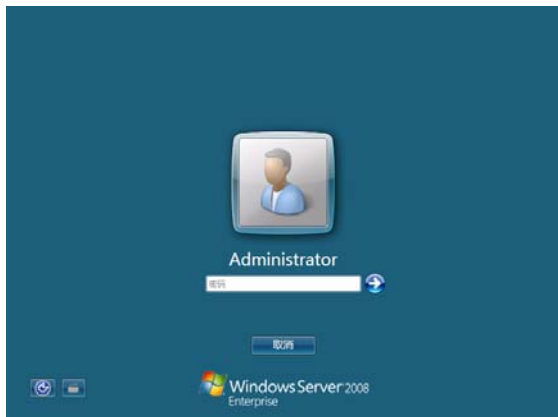


图 1-83 登录界面

16 在“密码”文本框中输入密码，按回车键即可登录 Windows Server 2008 系统桌面。默认自动启动“初始配置任务”窗口，如图 1-84 所示。

至此，Windows Server 2008 操作系统安装完成。



图 1-84 “初始配置任务”窗口

1.3.5 升级 Windows Server 2008

如果服务器中已安装 Windows Server 2003 系统，则可以直接升级到 Windows Server 2008，而且升级后的系统配置仍可保留。不过由于 Windows Server 2008 对服务器硬件配置的要求相对较高，因此必须保证服务器的硬件配置满足安装需求。

1 登录 Windows Server 2003，将 Windows Server 2008 光盘放入光驱自动运行，显示如图 1-85 所示的“安装 Windows”窗口。

② 单击“现在安装”按钮，安装程序开始检测本地系统配置。如果发现服务器配置不能满足安装需求，就会出现相应的提示。检测完成以后，显示如图 1-86 所示的“获取安装的重要更新”对话框。如果需要获取最新的更新以便成功安装 Windows，可单击“联机以获取最新安装更新（推荐）”按钮；否则单击“不获取最新安装更新”按钮。



图 1-85 “安装 Windows”窗口



图 1-86 “获取安装的重要更新”对话框

③ 单击“不获取最新安装更新”按钮，显示如图 1-87 所示的“选择要安装的操作系统”对话框，在列表框中可以选择待安装的操作系统版本。

④ 单击“下一步”按钮，显示如图 1-88 所示“请阅读许可条款”对话框，选中“我接受许可条款”复选框接受许可条款。

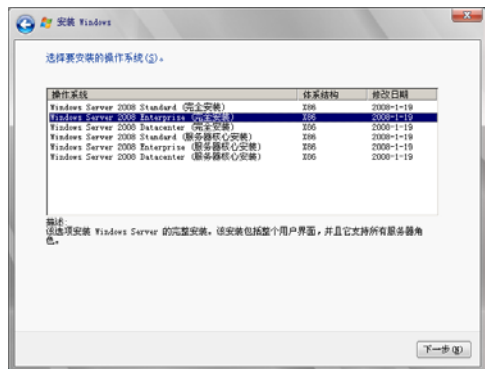


图 1-87 “选择要安装的操作系统”对话框



图 1-88 “请阅读许可条款”对话框

⑤ 单击“下一步”按钮，显示如图 1-89 所示的“您想进行何种类型的安装？”对话框。此时“升级”按钮为可用状态，用来升级到 Windows Server 2008。

⑥ 单击“升级”按钮，显示如图 1-90 所示的“兼容性报告”对话框，其中列出已检测到的设备问题。为了保证升级后的系统能够顺利运行，应仔细阅读该兼容性报告，并解决不兼容性问题。



图 1-89 “您想进行何种类型的安装？”对话框



图 1-90 “兼容性报告”对话框

⑦ 单击“下一步”按钮，开始复制文件并安装。安装完成以后，使用原来在 Windows Server 2003 中设置的用户账户和密码即可登录。具体步骤请参阅前面的相关内容，这里不再赘述。

1.3.6 添加与管理网络服务

在 Windows Server 2008 系统中采用“服务器管理器”替代了 Windows Server 2003 中的“管理您的服务器”，并且原来需要在“添加/删除 Windows 组件”和“配置您的服务器向导”来完成的操作都可以在“服务器管理器”中完成。

1. 添加服务器角色

Windows Server 2008 虽然比 Windows Server 2003 支持更多的网络服务，但默认并没有安装任何网络服务组件。它只提供了一个用户登录的独立网络服务器，而所有角色都可以通过“服务器管理器”添加。

① 单击“开始”→“管理工具”→“服务器管理器”选项，或者单击“开始”→“服务器管理器”选项，显示如图 1-91 所示的“服务器管理器”窗口。

提示

当关闭“初始配置任务”窗口时，系统也会自动打开“服务器管理器”窗口。



图 1-91 “服务器管理器”窗口

② 在“角色摘要”选项区域中单击“添加角色”超级链接，启动“添加角色向导”。首先显示如图 1-92 所示的“开始之前”对话框，其中列出可以完成的工作，以及操作之前的注意事项。

提示

也可以在“初始配置任务”窗口中单击“添加角色”超级链接，启动“添加角色向导”。

③ 单击“下一步”按钮，显示如图 1-93 所示的“选择服务器角色”对话框，在“角色”列表框中列出了所有可以安装的网络服务。如果需要安装哪种服务，只需选中相应的复选框即可。

④ 单击“下一步”按钮，开始安装所选服务。根据系统提示，部分网络服务安装过程中可能需要提供 Windows Server 2008 安装光盘。

2. 添加角色服务

服务器角色的模块化是 Windows Server 2008 的一个突出特点，在安装某些角色时还会安装一些扩展组件，用户完全可以根据自己的需要酌情选择。执行如下操作步骤添加其他角色服务。

① 打开如图 1-94 所示的“服务器管理器”窗口，并展开“角色”。选择已经安装的服务，例如

“路由和远程访问服务”。

② 在“角色服务”选项区域中单击“添加角色服务”超级链接，显示如图 1-95 所示的“选择角色服务”对话框，选择待添加的角色服务。



图 1-92 “开始之前”对话框

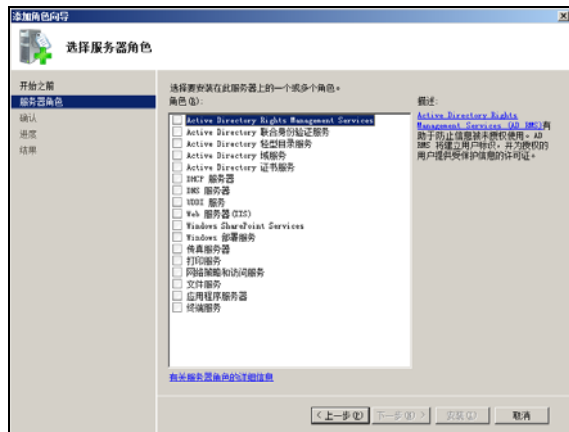


图 1-93 “选择服务器角色”对话框

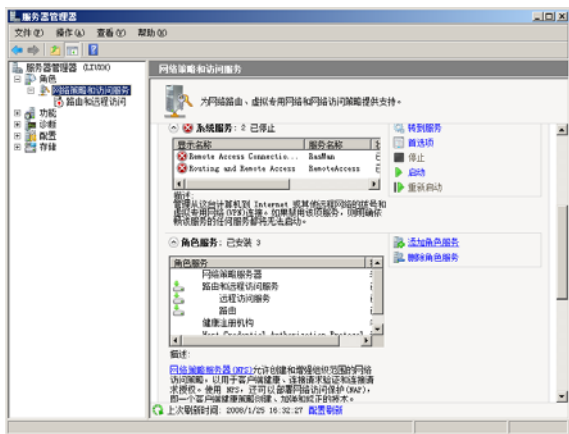


图 1-94 “服务器管理器”窗口



图 1-95 选择角色服务

③ 单击“下一步”按钮，开始安装相应的服务。

3. 删除服务器角色

删除之前应确认是否有其他网络服务或 Windows 功能需要调用当前服务，以免删除之后造成服务器瘫痪。

① 在“管理您的服务器”窗口中展开“角色”，显示已经安装的服务角色，如图 1-96 所示。

② 单击“删除角色”链接，显示如图 1-97 所示的“删除服务器角色”对话框，清除要删除角色前的复选框。

提示



删除角色服务，同样需要在指定服务器角色的管理器窗口中完成，单击“角色服务”选项旁边的“删除角色”超级链接即可。

③ 单击“下一步”按钮，删除所选角色。

4. 管理网络服务

Windows Server 2008 的网络服务管理更加智能化，大多数服务器角色都可以通过控制台直接管理。最简单的方法就是在“服务器管理器”窗口中展开角色并单击相应的服务器角色开始管理，如图 1-98 所示。

除此之外，也可以通过单击“开始”→“管理工具”选项并从中选择想要管理的服务器角色来打开单独的控制台窗口，配置和管理该服务器。

5. 添加和删除功能

Windows Server 2008 操作系统虽然功能强大，但许多功能需要特殊硬件配置支持。因此默认安装过程中不会添加任何扩展功能，需要用户自行选择添加。



图 1-96 已安装的服务角色



图 1-97 删除服务器角色

在“初始配置任务”窗口中单击“配置此服务器”选项区域中的“添加功能”超级链接，打开如图 1-99 所示的“添加功能向导”对话框。选中待安装功能组件前的复选框，然后单击“安装”或“下一步”按钮即可。

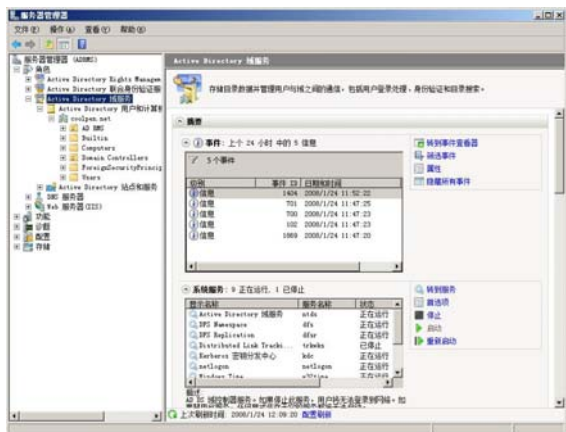


图 1-98 管理网络服务



图 1-99 添加功能向导

除此之外，同样可以在“服务器管理器”窗口中添加或删除 Windows 功能组件。在“服务器管理器”窗口中打开如图 1-100 所示的“功能摘要”窗口，在其中可以配置和管理已经安装的 Windows 功能组件。单击“添加功能”超级链接即可启动添加功能向导，选择要添加的功能即可。单击“删除功能”链接，打开“删除功能向导”。选择已经安装，但又不需要的功能将其删除即可。

1.3.7 Windows Server 2008 控制台

和 Windows Server 2003 系统一样，Windows Server 2008 系统也集成了控制台功能。并且为 3.0 版本，可以用来管理各种服务。原来基于 Web 或单独应用程序等方式的系统工具，在 Windows Server 2008 中都可以通过控制台来实现。控制台的使用方法如下。

- ① 运行“mmc”命令，打开控制台窗口，如图 1-101 所示。



图 1-100 功能摘要

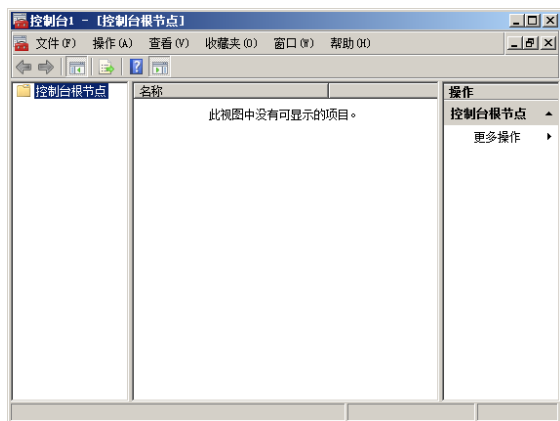


图 1-101 控制台窗口

② 单击“文件”→“添加/删除管理单元”选项，显示如图 1-102 所示的“添加/删除管理单元”对话框。在“可用的管理单元”下拉列表框中选择需要添加的管理单元，单击“添加”按钮添加到“所选管理单元”列表中，可以添加多个管理单元。

提示 有些组件在添加时会提示选择所管理的对象为本地计算机，还是远程计算机。

③ 单击“确定”按钮，将所选管理单元添加到控制台窗口中，如图 1-103 所示。此时，即可管理这些组件。

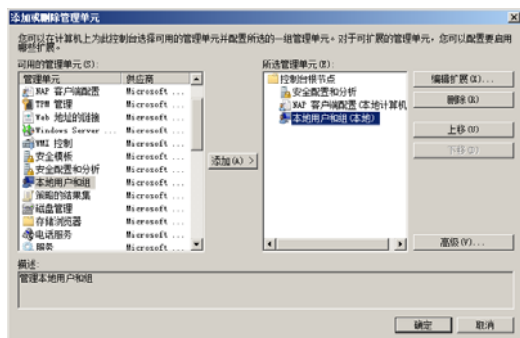


图 1-102 “添加/删除管理单元”对话框



图 1-103 添加的管理单元

1.3.8 Windows Server 2008 系统设置

在安装完成 Windows Server 2008 后，应设置计算机名、IP 地址，并且配置自动更新等，这些均可在“初始配置任务”或“服务器管理器”中完成。

1. 更改计算机名

Windows Server 2008 系统在安装过程中不需要设置计算机名，而是使用由系统随机配置计算机名。但系统配置的计算机名不仅冗长，而且不便于标记。因此为了更好地标识和识别服务器，应更改为易记或有一定意义的名称。

① 在“服务器管理器”窗口中的“计算机信息”选项组中单击“更改系统属性”超级链接，显示如图 1-104 所示的“系统属性”对话框。

提示 如果“服务器管理器”已关闭，可单击“开始”→“管理工具”→“服务器管理器”选项将其重新打开。



② 单击“更改”按钮，显示如图 1-105 所示的“计算机名/域更改”对话框，在“计算机名”文本框中输入一个新的计算机名。

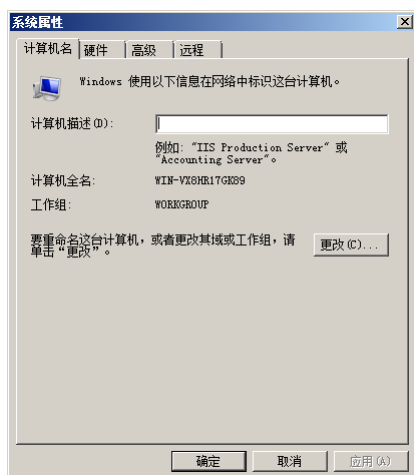


图 1-104 “系统属性”对话框

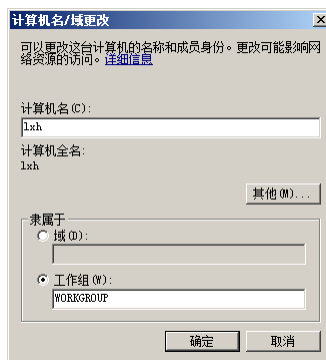


图 1-105 “计算机名/域更改”对话框

③ 单击“确定”按钮，显示如图 1-106 所示的“计算机名/域更改”提示框，提示必须重新启动计算机才能应用更改。

④ 单击“确定”按钮，显示如图 1-107 所示的提示框，提示必须重新启动计算机以应用更改。

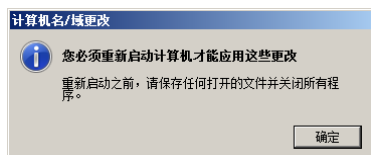


图 1-106 “计算机名/域更改”提示框

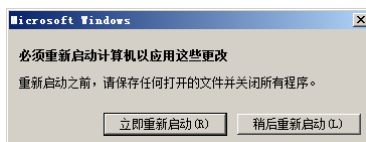


图 1-107 “重新启动”提示框

⑤ 单击“立即重新启动”按钮，重新启动系统并应用新的计算机名。

2. 设置 IP 地址

如果网络中安装有 DHCP 服务器，使用默认的“自动获得 IP 地址”即可；否则需要手动指定 IP 地址。

① 右击桌面状态栏托盘区域中的网络连接图标，选择快捷菜单中的“网络和共享中心”选项打开如图 1-108 所示的“网络和共享中心”窗口，其中显示网络连接状态。

② 在“任务”列表中单击“管理网络连接”超级链接，显示如图 1-109 所示的“网络连接”窗口。



图 1-108 “网络和共享中心”窗口

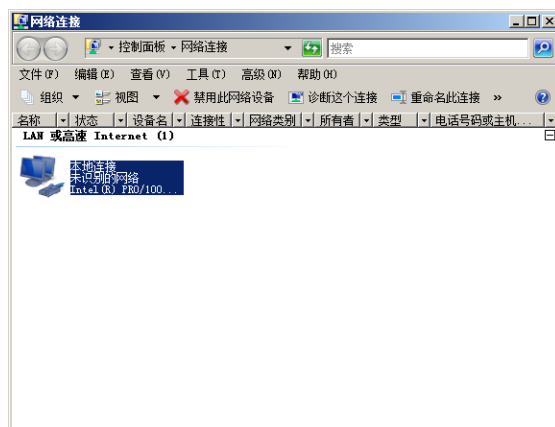


图 1-109 “网络连接”窗口

提示

也可以在“初始配置任务”窗口中单击“配置网络”超级链接打开“网络连接”窗口。

- ③ 右击“本地连接”图标，显示如图 1-110 所示的“本地连接 属性”对话框。

提示

由于现在主要使用 IPv4，IPv6 尚未正式使用。因此建议清除“Internet 协议版本 6 (TCP/IPv6)”复选框，只使用 IPv4 地址。

- ④ 选中“Internet 协议版本 4 (TCP/IPv4)”选项，单击“属性”按钮，显示如图 1-111 所示的“Internet 协议版本 4 (TCP/IPv4) 属性”对话框。如果要手动指定 IP 地址，可选择“使用下面的 IP 地址”和“使用下面的 DNS 服务器地址”单选按钮，并输入 IP 地址、子网掩码、默认网关、首选 DNS 服务器和备用 DNS 服务器等。

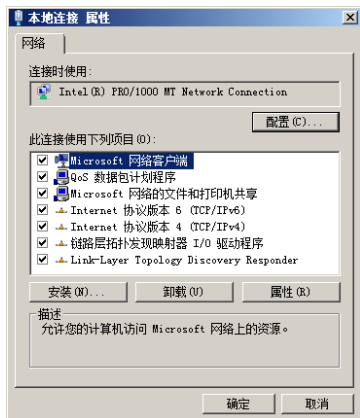


图 1-110 “本地连接 属性”对话框

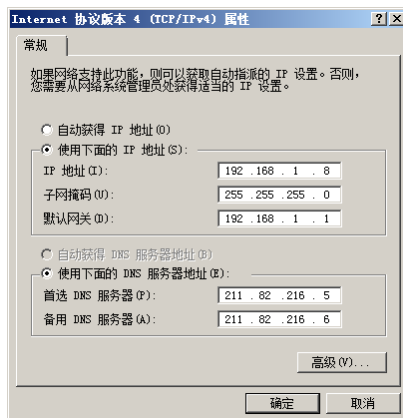


图 1-111 “Internet 协议版本 4 (TCP/IPv4) 属性”对话框

- ⑤ 单击“确定”按钮。

3. 设置自动更新

为了增加系统功能，避免因漏洞而造成故障，必须启动自动更新功能及时下载并安装更新程序，以保护系统的安全。

- ① 在“服务器管理器”窗口的“安全信息”选项区域中单击“配置更新”超级链接，显示如图 1-112 所示的“Windows Update”对话框。

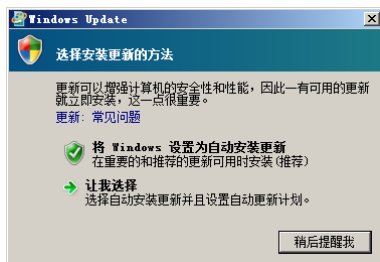


图 1-112 “Windows Update”对话框

提示

只有第 1 次配置自动更新时才会显示该对话框，以后将不再显示。

- ② 如果要让系统设置为自动安装更新，则单击“让 Windows 设置为自动安装更新”按钮；如果要手动配置，则单击“让我选择”按钮，显示 1-113 所示的“更改设置”窗口，在“选择 Windows 安装更新的方法”中选择一种安装方法即可。

- ③ 单击“确定”按钮保存设置，再次在“服务器管理器”窗口中单击“配置更新”超级链接，

显示如图 1-114 所示的“Windows Update”窗口。

④ 单击“检查更新”按钮，Windows Server 2008 根据所做配置自动从 Windows Update 网站检测并下载更新。



图 1-113 “更改设置”窗口



图 1-114 “Windows Update”窗口

第 2 章 Server Core

Windows Server 2008 Server Core 即 Windows Server 2008 服务器核心，它是微软公司推出的改进非常大的功能组件。Server Core 没有图形界面，仅以命令行运行，并且只提供特定功能的 Windows 核心基础服务。该组件以安全性及稳定性为第一要务，从而减少其他服务和管理工具可能受到的攻击。

2.1 概述

Server Core 类似于 Linux 和 UNIX，由于只安装了系统核心基础服务，因此更加安全可靠。并且减少了被攻击的可能性，同时也降低了管理的复杂度。它实现有限的服务器角色，例如文件服务器、DHCP 服务器、DNS 服务器和 AD DS 服务等。从而能够有效地提高安全性和降低管理复杂度，也可以实现更高的稳定性。

2.1.1 Server Core 的优点

Windows Server 2008 Server Core 主要具备以下优点。

(1) 服务器的稳定性更高：由于 Server Core 安装的功能较少，并且只用来运行很少的服务和应用，因此系统漏洞和占用的资源也更少。与运行了更多功能的服务器相比，极大地提高了服务器的稳定性和性能。

(2) 减少软件维护量：由于 Server Core 只安装最基本的功能，因此所需管理的软件也就更少。从而提高了管理性，降低了软件维护量。例如，需要更新和安装补丁的软件更少。

(3) 降低被攻击风险：服务器只安装有限的服务和应用，因此暴露在网络中的攻击点也很有限。从而使攻击者的攻击面更少，在很大程度上降低了被攻击的可能性。

(4) 空间占有率更少：Server Core 没有安装不必要的驱动、应用和图形界面，因此安装后只占用 1 GB 左右的磁盘空间，是正常 Windows Server 2008 的 1/6。并且安装完成之后，由于运行的程序很少，所以对服务器的资源占有率也大大降低。同时只有需要角色的文件才会被安装，而不会安装 IE 及 .NET 框架等。

提示

Server Core 中的命令不区分大小写。

2.1.2 Server Core 的缺点

由于 Server Core 的管理全部使用命令行完成，因此对于已经熟悉 Windows 图形化界面的网络管理员来说难度比较大。即不仅需要熟悉命令行模式下的管理模式，同时更要记住复杂的命令。

2.2 安装 Server Core

安装 Windows Server 2008 Server Core 可以使用安装盘安装，只是在安装过程中需要选择不同版本。安装完成以后，所有服务的安装、配置及关机操作都要在命令提示符下完成。

2.2.1 安装 Server Core

安装 Server Core 的步骤如下。

① 使用 Windows Server 2008 安装光盘启动计算机，运行安装程序，显示如图 2-1 所示的安装界面。在其中可以选择安装语言、时间、键盘和输入方法等，使用默认设置即可。

② 单击“下一步”按钮，显示如图 2-2 所示的界面，提示即将安装。



图 2-1 安装界面



图 2-2 提示即将安装

③ 单击“现在安装”按钮，显示如图 2-3 所示的“选择您购买的 Windows 版本”对话框。在“Windows 版本”列表中选择待安装的 Server Core 版本，例如“Windows Server 2008 Enterprise（服务器核心安装）”选项。

④ 单击“下一步”按钮，显示如图 2-4 所示的“请阅读许可条款”对话框。选中“我接受许可条款”复选框，接受许可条款。

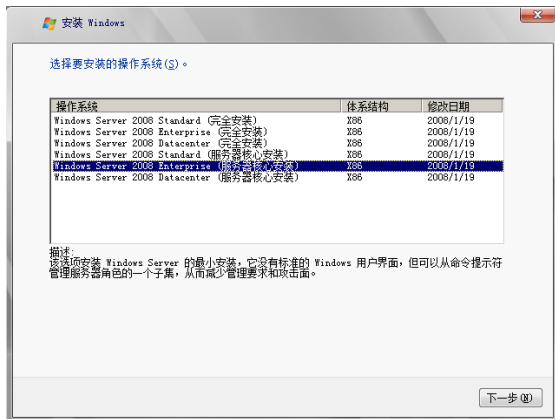


图 2-3 “选择您购买的 Windows 版本”对话框

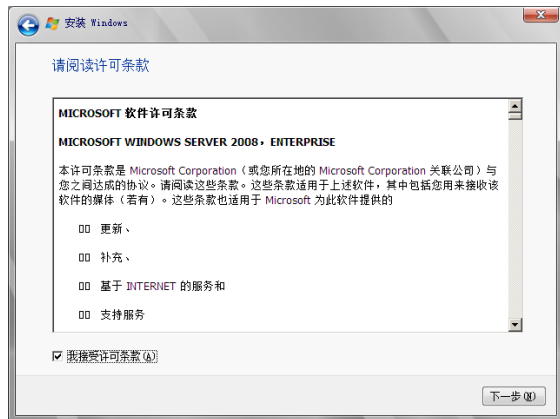


图 2-4 “请阅读许可条款”对话框

⑤ 单击“下一步”按钮，显示如图 2-5 所示的“您想进行何种类型的安装”对话框。由于服务器中没有安装任何操作系统，因此“升级”模式不能使用。

⑥ 单击“自定义（高级）”按钮，显示如图 2-6 所示的“您想将 Windows 安装在何处”对话框。在其中选择目标安装磁盘，这里只有一块硬盘并且还没有分区。

⑦ 单击“驱动器选项”按钮，显示如图 2-7 所示的硬盘操作界面，在其中可以执行分区及格式化硬盘等操作。

⑧ 如果需要分区硬盘，单击“新建”按钮。显示如图 2-8 所示的分区硬盘界面，在“大小”文本框中输入新分区的大小。



图 2-5 “您想进行何种类型的安装”对话框



图 2-6 “您想将 Windows 安装在何处”对话框



图 2-7 硬盘操作界面



图 2-8 分区硬盘界面

⑨ 单击“应用”按钮，一个分区划分成功，如图 2-9 所示。选择剩余的未分配空间，单击“新建”按钮可继续划分其他分区。

⑩ 选择待安装操作系统的分区，单击“下一步”按钮。开始安装 Server Core，如图 2-10 所示。

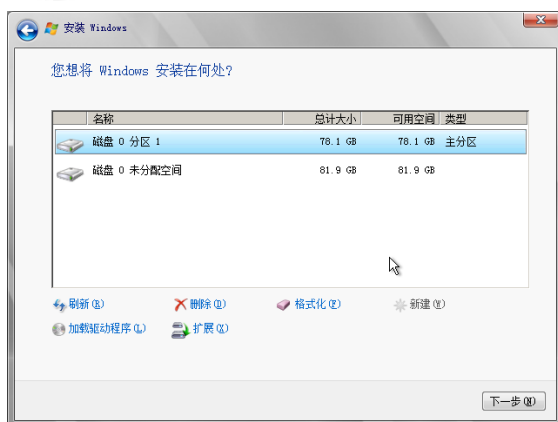


图 2-9 第 1 个分区成功



图 2-10 开始安装

⑪ Server Core 安装完成后会自动重新启动计算机，显示如图 2-11 所示的提示登录界面，提示需要按 Ctrl+Alt+Delete 组合键登录。

⑫ 按 Ctrl+Alt+Delete 组合键，显示如图 2-12 所示的选择用户界面。



图 2-11 提示登录界面

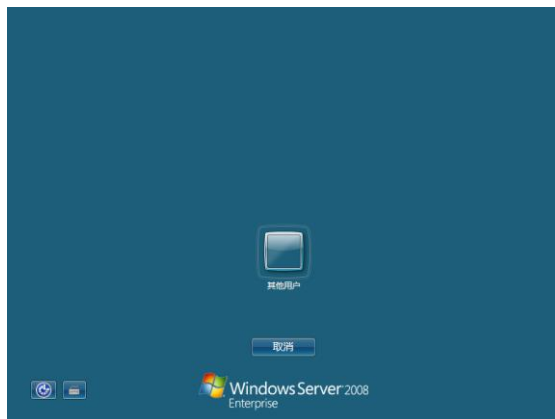


图 2-12 选择用户界面

⑬ 单击“其他用户”按钮，显示如图 2-13 所示的输入用户名和密码界面，提示输入用户名和密码。

⑭ 在“用户名”文本框中输入管理员用户名 administrator，按回车键，显示如图 2-14 所示的界面更改密码界面，提示更改密码。

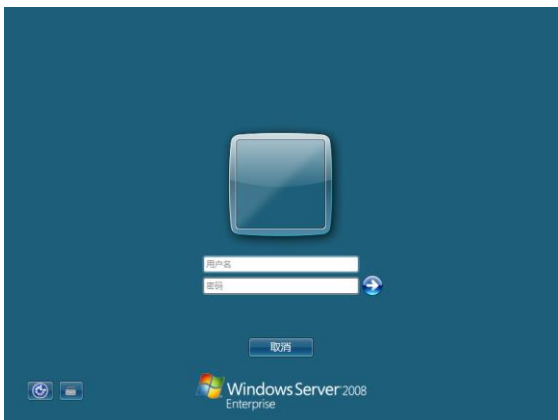


图 2-13 提示输入用户名和密码

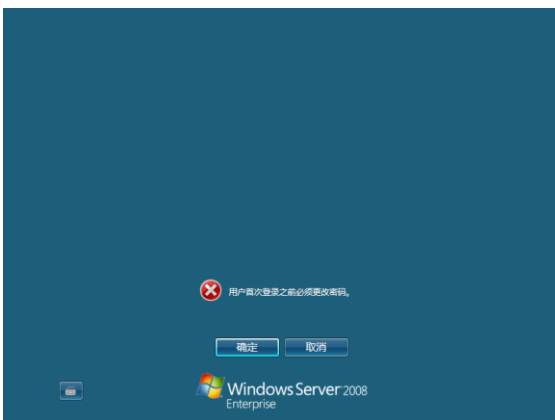


图 2-14 更改密码界面

⑮ 单击“确定”按钮，显示如图 2-15 所示的设置新密码界面，在其中可以设置新密码。

⑯ 在“新密码”和“确认密码”文本框中输入一个新密码，按回车键，提示密码已更改，如图 2-16 所示。以后登录系统时，可使用此处设置的密码。

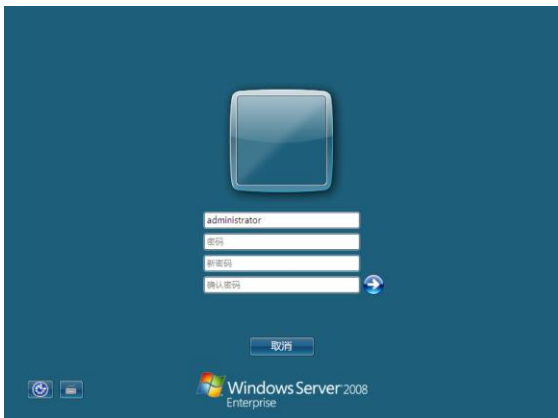


图 2-15 设置新密码界面

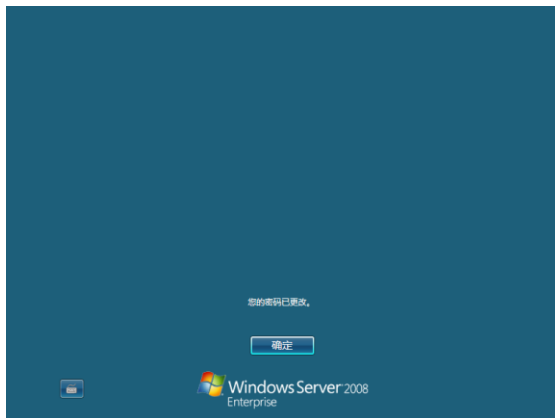


图 2-16 提示密码已更改

⑰ 单击“确定”按钮，即可登录 Server Core。并且显示命令提示符窗口，如图 2-17 所示。

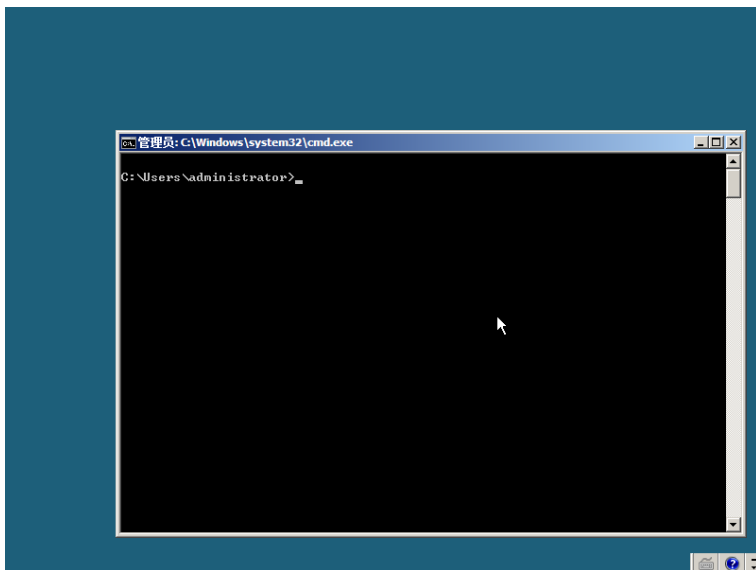


图 2-17 命令提示符窗口

至此，Server Core 安装完成，所有的服务配置均在该命令提示符窗口中完成。

2.2.2 服务器关机

由于 Windows Server 2008 Server Core 中没有图形界面，因此无法像普通 Windows 一样通过“开始”菜单来关机、注销和重新启动，需要使用 Shutdown 命令来实现这些操作。

shutdown 命令的语法格式为：

```
shutdown [/i | /l | /s | /r | /g | /a | /p | /h | /e] [/f] [/m \\computer] [/t xxx] [/d [p|u:]xx:yy [/c "comment"]]
```

常用参数说明如下。

- (1) /?: 显示帮助信息。
- (2) /l: 注销当前账户。
- (3) /s: 关闭计算机。
- (4) /r: 关闭并重新启动计算机。
- (5) /g: 关闭并重新启动计算机，系统重新启动后启动所有注册的应用程序。
- (6) /t xxx: 设置关闭前的超时为 xxx 秒，有效范围为 0~600，默认为 30。默认已设置 /f 参数。
- (7) /a: 中止系统关闭，但只能在超时期间内使用。
- (8) /c "comment" : 注释重新启动或关闭的原因，最多允许 512 个字符。
- (9) /f: 强制关闭正在运行的应用程序，且不出现警告。使用 /t xxx，默认使用 /f。



注意：

在使用/s或/r等命令关闭或重新启动系统时，如果未加/t xxx参数，则默认延时时间为1分钟。



例如，现在要关闭计算机，可在命令提示符中输入如下命令：

```
Shutdown /s
```

按回车键，显示如图 2-18 所示的“您将要被注销”对话框，提示 Windows 将在 1 分钟内关闭。1 分钟之后，系统就会自动关闭。



注意：

如果此时单击“关闭”按钮，虽然可关闭该对话框，但并不中止关机过程，该过程仍在后台运行。



如果要在 10 分钟以后让系统自动重新启动，则可在命令提示符窗口中输入如下命令：

```
Shutdown /s /t 600
```

按回车键，显示如图 2-19 所示“您将要被注销”对话框，提示 Windows 将在 10 分钟内关闭。10 分钟后，系统就会自动关机。



图 2-18 “您将要被注销”对话框

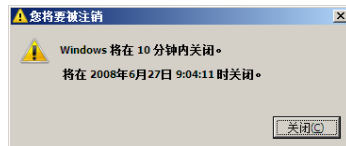


图 2-19 “您将要被注销”对话框

2.3 重命名服务器

在安装 Windows Server 2008 时不需要用户设置计算机名，系统会随机生成一个计算机名，Server Core 也是如此。

使用 hostname 命令，可以查看当前计算机名，而重命名则需使用 netdom 命令。

① 在命令提示符下输入如下命令：

```
hostname
```

按回车键，显示当前的计算机名，如图 2-20 所示。

② 使用 Netdom 命令来更改计算机名，格式为：

```
netdom renamecomputer 旧服务器名称 /Newname:新服务器名称
```

例如：

```
netdom renamecomputer WIN-Y80UAHMI1RBQ /newname:lxh
```

按回车键，显示如图 2-21 所示的信息。提示重命名计算机可能导致某些服务不能正确运行，并询问是否要继续。

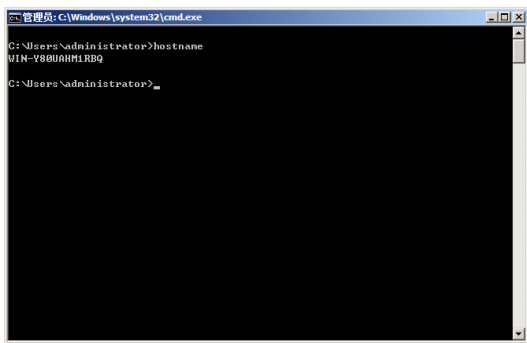


图 2-20 当前计算机名

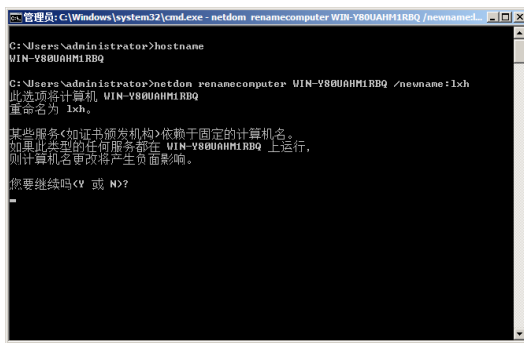


图 2-21 重命名计算机提示信息

③ 输入 y，按回车键，命令成功完成，如图 2-22 所示。重新启动系统后新计算机名才能生效。

④ 运行 shutdown 命令重新启动计算机。为了加快关机速度，可设置关机延时为 2 秒。在命令提示符下输入如下命令：

```
shutdown /r /t 2
```

按回车键，重新启动计算机并登录，即可应用新的计算机名。

2.4 设置 IP 地址

安装完成 Server Core 后，默认使用以 DHCP 的模式分配 IP 地址。由于服务器通常使用静态 IP 地址，因此需要在安装后为系统设置静态 IP 地址，为此使用 netsh 命令。这里设置服务器的 IP 地址为 211.82.216.2，子网掩码为 255.255.255.192，网关为 211.82.216.62，DNS 服务器为 202.99.160.68。

① 在命令提示符下输入如下命令：

```
netsh interface ipv4 show interfaces
```

按回车键，显示如图 2-23 所示的服务器中可用的网络连接信息，本地连接的 ID 为 2。

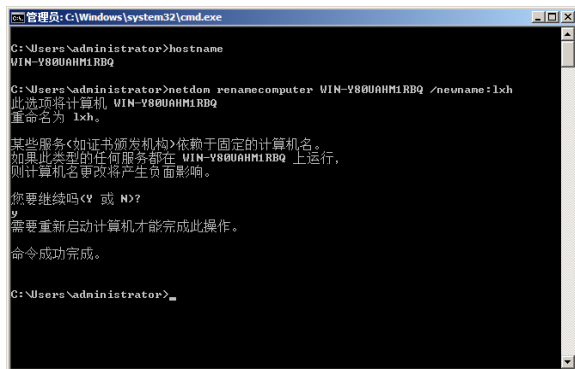


图 2-22 成功完成重命名

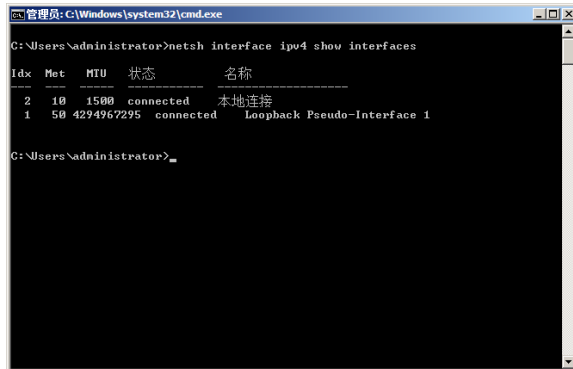


图 2-23 网络连接信息

② 在命令提示符下输入如下命令：

```
netsh interface ipv4 set address name="2" source=static address="211.82.216.2" mask="255.255.255.192" gateway="211.82.216.62"
```

按回车键，设置服务器的 IP 地址为 211.82.216.2，子网掩码为 255.255.255.192，网关为 211.82.216.62，如图 2-24 所示。

③ 在命令提示符下输入如下命令：

```
netsh interface ipv4 add dnsserver name="2" address="202.99.160.68" index=1
```

按回车键，将服务器的首选 DNS 服务器设置为 202.99.160.68，如图 2-25 所示。

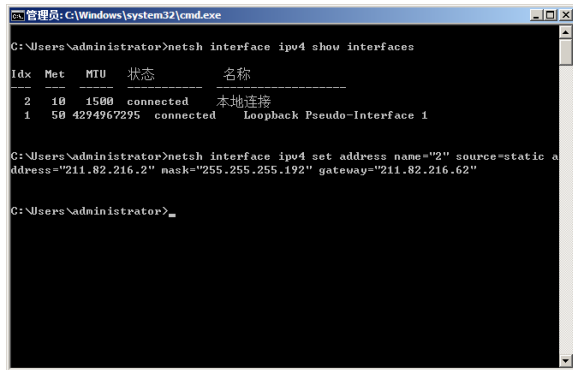


图 2-24 设置 IP 地址

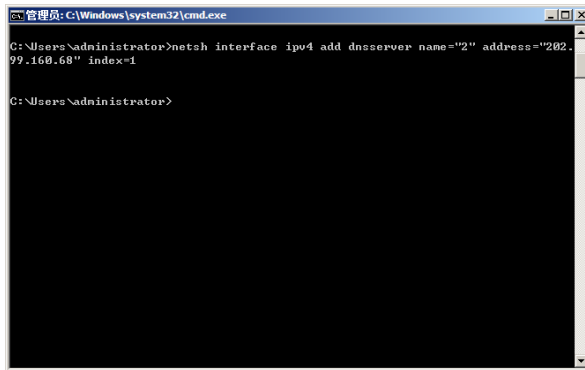


图 2-25 设置 DNS 服务器

2.5 安装 AD DS 域服务

AD DS 域服务是网络基础服务组件，需要使用 dcpromo 命令。将服务器提升为域控制器，而且必须使用无人职守安装文件模式。

2.5.1 无人职守安装文件

安装域服务之前，必须首先创建无人职守安装文件，然后利用 U 盘等移动设备将该文件复制到 Server Core 服务器的本地磁盘中。例如，现在要将服务器升级为域控制器，并且 DNS 域名为“coolpen.net”，则无人职守安装文件内容如下：

```
[DCInstall]
; New forest promotion
ReplicaOrNewDomain=Domain
NewDomain=Forest
NewDomainDNSName=coolpen.net
ForestLevel=0
DomainNetbiosName=COOLPEN
DomainLevel=0
InstallDNS=Yes
ConfirmGc=Yes
CreateDNSDelegation=No
DatabasePath="C:\Windows\NTDS"
LogPath="C:\Windows\NTDS"
SYSVOLPath="C:\Windows\SYSVOL"
; Set SafeModeAdminPassword to the correct value prior to using the unattend file
SafeModeAdminPassword="abcde_123"
; Run-time flags (optional)
; RebootOnCompletion=Yes
```

其中几个比较重要的参数说明如下。

- (1) **NewDomainDNSName**：设置域的 DNS 域名。
- (2) **DomainNetbiosName**：设置 NetBIOS 名称。
- (3) **DatabasePath**：设置域控制器的数据库保存路径。
- (4) **LogPath**：设置域控制器数据库的日志保存路径。
- (5) **SafeModeAdminPassword**：设置目录还原模式密码，并且必须为强密码。

如果要将服务器升级为域 coolpen.net 子域，子域名称为“book.coolpen.net”，则无人职守安装文件的内容如下：

```
[DCInstall]
; New child domain promotion
ReplicaOrNewDomain=Domain
NewDomain=Child
ParentDomainDNSName=coolpen.net
ChildName=book
DomainNetbiosName=BOOK
DomainLevel=0
SiteName=Default-First-Site-Name
InstallDNS=Yes
ConfirmGc=Yes
CreateDNSDelegation=Yes
DNSDelegationUserName=coolpen.net\administrator
DNSDelegationPassword=*
UserDomain=coolpen.net
UserName=coolpen.net\administrator
Password=*
DatabasePath="C:\Windows\NTDS"
LogPath="C:\Windows\NTDS"
SYSVOLPath="C:\Windows\SYSVOL"
; Set SafeModeAdminPassword to the correct value prior to using the unattend file
```

```
SafeModeAdminPassword="abcde_123"
; Run-time flags (optional)
; RebootOnCompletion=Yes
```

其中几个重要参数的说明如下。

- (1) ParentDomainDNSName: 设置父域的 DNS 域名。
- (2) ChildName=book: 设置子域名称。
- (3) DomainNetbiosName: 设置子域的 NetBIOS 名称。
- (4) DNSDelegationUserName: 设置具有加入子域权限的用户账户名。
- (5) DNSDelegationPassword: 设置具有加入子域权限的用户账户密码。
- (6) DatabasePath: 设置域控制器的数据库保存路径。
- (7) LogPath: 设置域控制器数据库的日志保存路径。
- (8) SYSVOLPath: 设置 SYSVOL 的保存路径。
- (9) SafeModeAdminPassword: 设置目录还原模式密码, 并且必须为强密码。

提示



在图形界面的 Windows Server 2008 中运行域服务安装向导时, 在如图 2-26 所示的“摘要”对话框中显示所做的配置。单击“导出设置”按钮, 可将设置参数导出到文本文件中, 然后相应的 DNS 域名即可应用于 Server Core。



图 2-26 “摘要”对话框

2.5.2 安装 AD DS 域服务

将无人值守安装文件复制到服务器中, 假设其文件名为“ad.txt”, 保存在 C 盘根目录下。

- ① 在命令提示符下运行 dcpromo 命令, 用于启动域服务安装过程:

```
dcpromo /unattend:d:\ad.txt
```

按回车键, 开始检查并验证环境和参数, 如图 2-27 所示。

验证完成以后开始安装域服务, 如图 2-28 所示。

安装完成以后, 系统自动重新启动, 安装完成域服务。

- ② 重新启动并登录以后查看当前安装的应用和尚未安装服务, 在命令提示符下输入如下命令:

```
Oclist
```

按回车键, 显示所有安装和未安装的服务信息, 如图 2-29 所示。

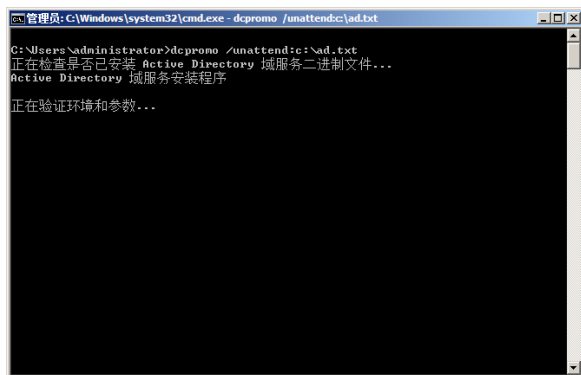


图 2-27 检查并验证环境和参数

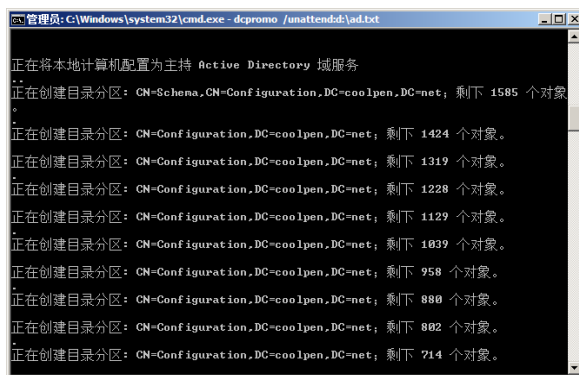


图 2-28 开始安装域服务

2.6 安装服务组件

Server Core 支持远程管理功能，可以在网络中的某台客户端上利用远程桌面进行远程管理。不过，需要首先在 Server Core 服务器上更改注册表设置，同时在防火墙中启用远程桌面端口后，客户端才能连接服务器。

2.6.1 启用远程管理

启用远程管理的步骤如下。

① 在 Server Core 服务器的命令提示符下输入如下命令：

```
cd c:\windows\system32
```

按回车键，进入系统目录。

② 在命令行提示符下输入如下命令：

```
cscript scregedit.wsf /ar 0
```

按回车键，更新注册表，如图 2-30 所示。

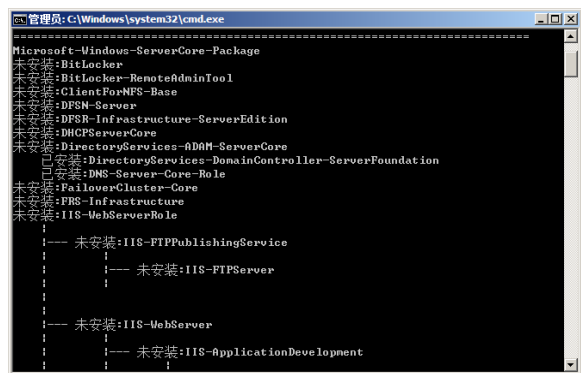


图 2-29 显示安装和未安装的服务信息

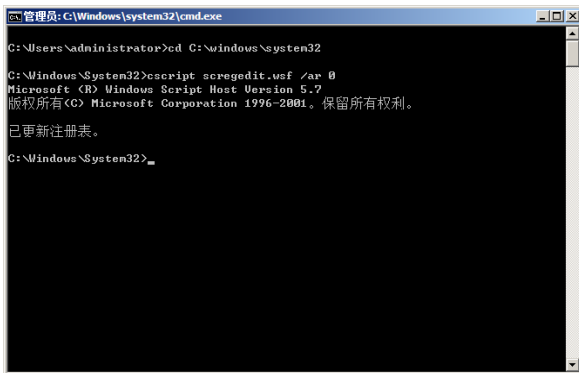


图 2-30 更新注册表

③ 在命令行提示符下输入如下命令：

```
slmgr.vbs -ato
```

按回车键，激活服务器，如图 2-31 所示。

④ 为了保证服务器和客户端能够正常连通，可利用 Ping 命令测试，在命令提示符下输入如下命令：

```
ping 211.82.216.16
```


按回车键，显示如图 2-32 所示信息，表示能够正常通信。

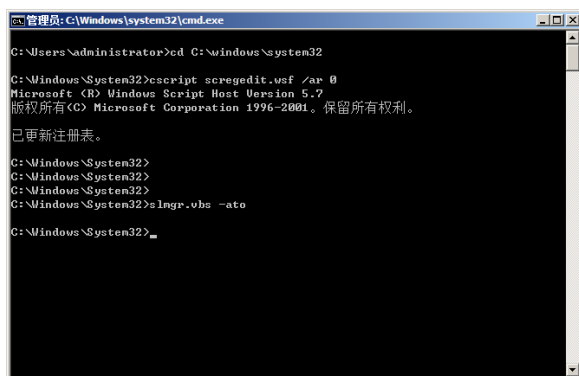


图 2-31 激活服务器

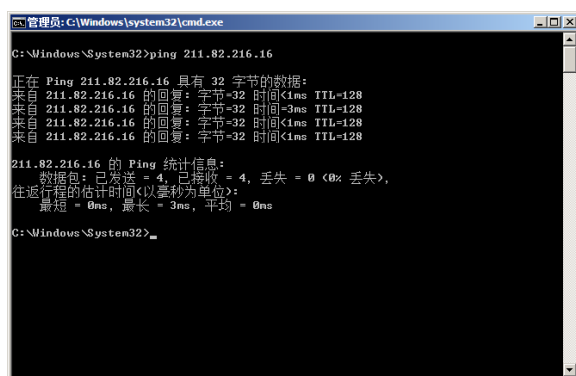


图 2-32 测试与客户端的连接

2.6.2 客户端连接

如果客户端具有远程桌面功能，即可远程登录 Server Core 服务器并进行管理。这里以 Windows Vista 为例。

① 在 Windows Vista 系统中单击“开始”→“所有程序”→“附件”→“远程桌面连接”选项，打开如图 2-33 所示的“远程桌面连接”对话框，在“计算机”文本框中输入 Server Core 服务器的 IP 地址。

② 单击“连接”按钮，显示如图 2-34 所示的“Windows 安全”对话框，分别在“用户名”和“密码”文本框中输入管理员账户和密码。

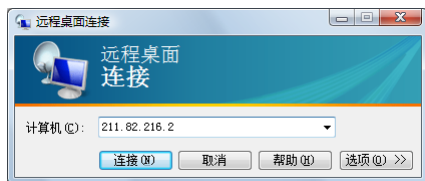


图 2-33 “远程桌面连接”对话框

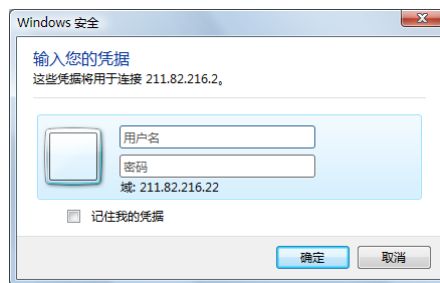


图 2-34 “Windows 安全”对话框

③ 单击“确定”按钮，远程登录到 Server Core 服务器。远程管理界面如图 2-35 所示，此时即可像在本计算机上一样进行管理。

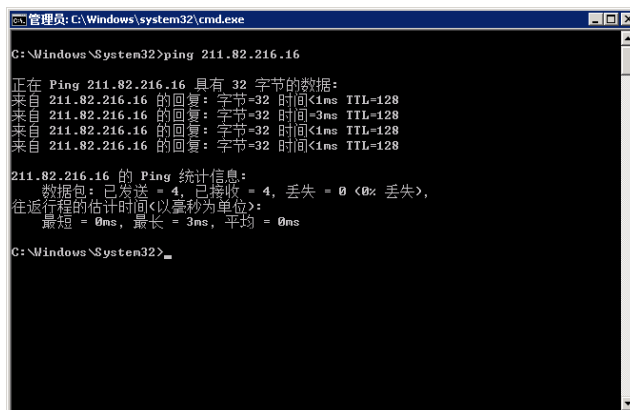


图 2-35 远程管理界面

2.7 用户与组管理命令

用户和组的管理是所有系统都经常用到的，Server Core 也是如此。用户和组的配置主要是在命令行模式下通过 Net 命令添加和删除，因此需要网络管理员熟悉各种命令的操作。

2.7.1 计算机账户管理——net computer

net computer 的功能是在域中添加或删除计算机账户。

1. 在域中添加计算机

要将计算机 hslhn 添加到域中，在命令提示符下输入如下命令：

```
net computer \\hslhn /add
```

按回车键，该计算机被添加到域中，如图 2-36 所示。

如果要将计算机 hslhn 从域中删除，则在命令提示符下输入如下命令：

```
net computer \\hslhn /del
```

按回车键，即可将计算机从域中删除，如图 2-37 所示。

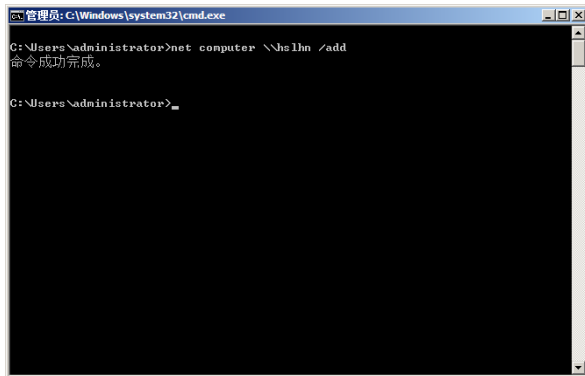


图 2-36 在域中添加计算机

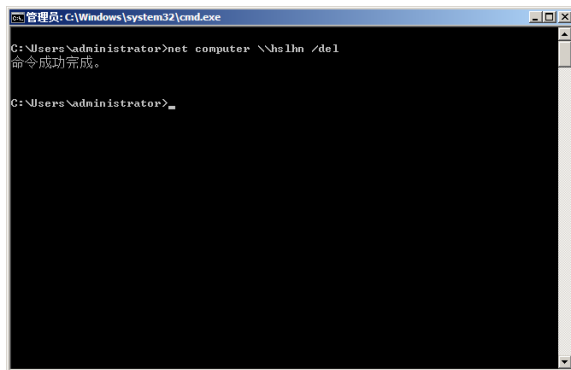


图 2-37 将计算机从域中删除

2. net computer 命令说明

net computer 命令的语法格式如下：

```
net computer \\ComputerName {/add | /del}
```

参数说明如下。

- (1) \\Computername: 指定要从域中添加或删除的计算机账户名称。
- (2) {/add | /del}: 指定从域中添加或删除指定的计算机。

2.7.2 用户账户管理——net user

net user 命令用于查看、添加设置及用户登录时间。

1. 查看用户账户

要查看本地计算机上所有的用户账户，在命令提示符下输入如下命令：

```
net user
```

按回车键，显示当前计算机中所有的用户账户，如图 2-38 所示，

要查看其中某个用户账户的详细信息，例如 Administrator，在命令提示符下输入如下命令：

```
net user administrator
```

按回车键，显示 Administrator 账户的详细信息。如用户名及所属的用户组等，如图 2-39 所示。

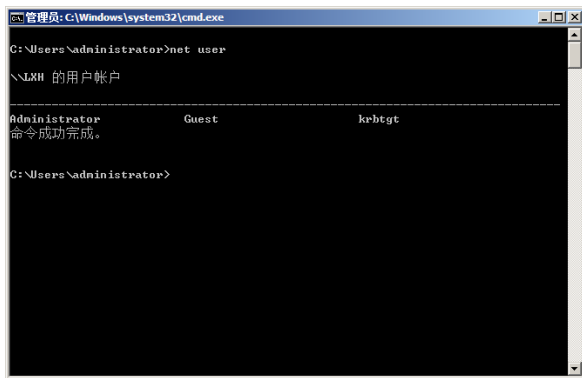


图 2-38 所有用户账户



图 2-39 Administrator 账户信息

2. 添加用户账户

例如，要添加一个用户账户 lhn，设置登录密码为“abcde_123”，用户全名为“lihaining”，在命令提示符下输入如下命令：

```
net user lhn abcde_123 /add /fullname:"lihaining"
```

按回车键，成功添加该用户账户，如图 2-40 所示。

在命令提示符下输入如下命令：

```
net user
```

按回车键，显示所有的用户账户。可以看到用户 lhn 已添加成功，如图 2-41 所示。

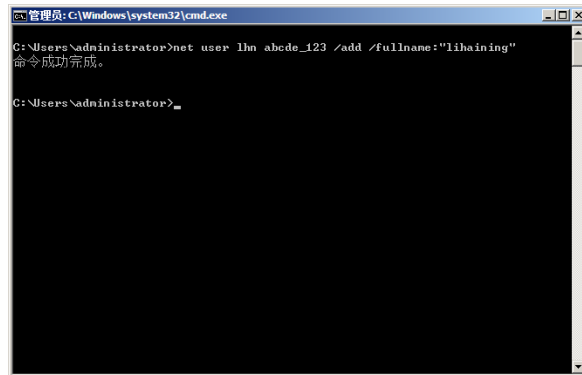


图 2-40 添加用户账户

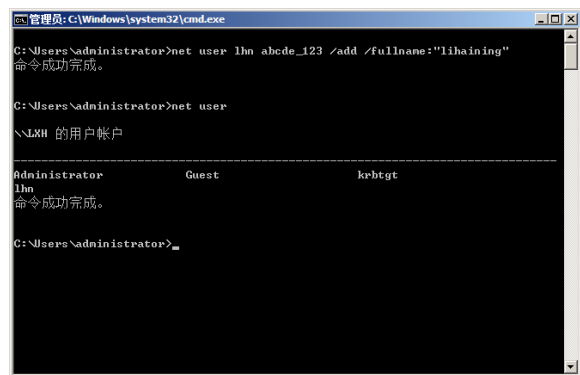


图 2-41 用户 lhn 已添加成功

如果要更改用户账户的密码，例如，将用户 lhn 的密码更改为“abc_1234”，在命令提示符下运行如下命令：

```
net user lhn abc_1234
```

3. 设置用户登录时间

要使用 24 小时制表示法设置用户 lhn 的登录时间为上午 8 点~下午 5 点，在命令提示符下输入如下命令：

```
net user lhn /time:M-F,08:00-17:00
```

按回车键，用户 lhn 只能在上午 8 点~下午 5 点的时间段内登录，如图 2-42 所示。

如果要详细指定用户的登录时间，例如，指定用户账户 lhn 的登录时间为星期一的上午 6 点~下午 5 点、星期六的下午 1 点~3 点，以及星期日的上午 8 点~下午 5 点。在命令提示符下输入如下命令：

```
net user lhn /time:M,6am-5pm;Sa,1pm-3pm;Su,8:00-17:00
```

按回车键，命令成功执行，如图 2-43 所示。

现在查看添加的用户账户 lhn 的详细信息，在命令提示符下输入如下命令：

```
net user lhn
```

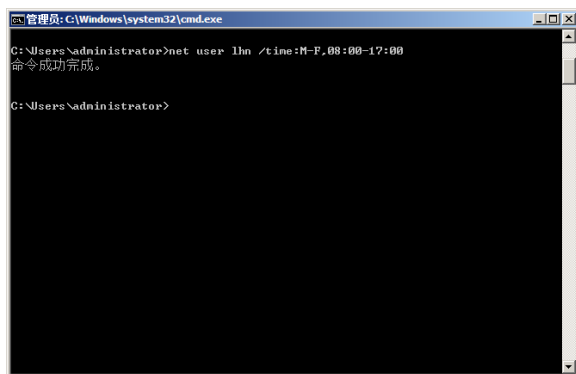


图 2-42 设置用户登录时间

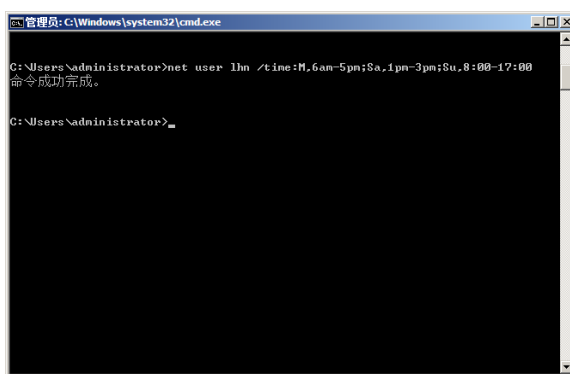


图 2-43 设置用户登录的详细时间

按回车键，显示用户账户 lhn 的详细信息，如图 2-44 所示，其中列出了用户名及登录时间等详细信息。

4. 禁用和启用账户

如果要禁用一个用户账户，例如，要禁用用户 liuxh，则在命令提示符下输入如下命令：

```
net user liuxh /active:no
```

按回车键，用户 liuxh 被禁用，如图 2-45 所示。

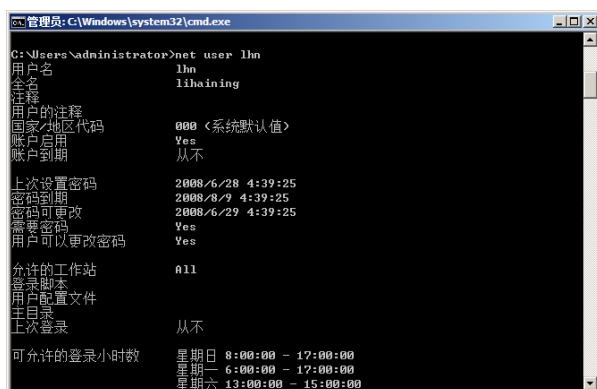


图 2-44 用户账户 lhn 的详细信息

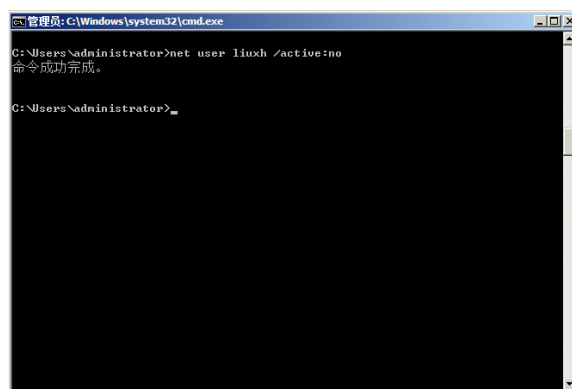


图 2-45 禁用用户账户 liuxh

如果要重新启动该账户，在命令提示符下输入如下命令：

```
net user liuxh /active:yes
```

5. net user 命令说明

net user 命令的语法格式为：

```
net user [username [password | *] [options]] [/DOMAIN]
net user username {password | *} /ADD [options] [/DOMAIN]
net user username [/DELETE] [/DOMAIN]
net user username [/TIMES:{times | ALL}]
```

参数说明如下。

- (1) **userName**: 指定要添加、删除、修改或查看的用户账户名。
- (2) **password**: 为用户账户设置密码。如果使用 *，则会提示输入密码，但不显示输入的内容。
- (3) **/domain**: 在计算机主域的主域控制器执行操作。

参数[options]中可以使用的有效命令行选项如表 3-1 所示。

表 3-1 [options]中可以使用的有效命令行选项

参数的语法格式	说 明
/active:{no yes}	启用或禁用用户账户。如果用户账户未启用，则其无法访问计算机中的资源，默认设置为 yes（即启用状态）
/comment:"text"	提供关于用户账户的描述性说明，最多可以有 48 个字符，为文本加上引号
/countrycode:nnn	使用操作系统“国家（地区）”代码为用户帮助和错误消息实现指定的语言文件，数值 0 代表默认的“国家（地区）”代码
/expires:{[mm/dd/yyyy dd/mm/yyyy mmm, dd, yyyy] never}	指定用户账户的过期日期，可以是[mm/dd/yyyy], [dd/mm/yyyy]或[mmm,dd,yyyy]格式，取决于国家（地区）代码。注意，账户在指定日期开始时到期。月份值可以使用数字、全称或 3 个字母的缩写（即 Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov 和 Dec）；年份值可以使用两位数或 4 位数。使用逗号和斜杠分隔日期的各部分，不要使用空格。如果省略 yyyy，将假定为下一次出现的日期（根据计算机的日期和时间而定）。例如，如果输入的日期在 1998 年 1 月 10 日~1999 年 1 月 8 日之间，则下列日期项相等： jan,9 1/9/99 january,9,1999 1/9
/fullname:"name"	指定用户的全名而不是用户名，将名称用引号引起
/homedir:Path	设置用户主目录的路径。该路径必须存在
/passwordchg:{yes no}	指定用户是否可以更改自己的密码，默认设置为 yes
/passwordreq:{yes no}	指定用户账户是否必须有密码，默认设置为 yes
/profilepath:[Path]	设置用户登录配置文件的路径，该路径指向注册表配置文件
/scriptpath:Path	设置用户登录脚本的路径，不能是绝对路径，而是 %systemroot%\System32\Repl\Import\Scripts 的相对路径
/times:{day[-day][,day[-day]] .time[-time][,time[-time]] [; all]}	指定用户可以使用计算机的时间，增加值限制为 1 小时。day 值可以用全称或缩写（即 M、T、W、Th、F、Sa 及 Su）。可以使用 12 小时或 24 小时时间表示法，12 小时表示法使用 AM、PM 或 A.M.、P.M.。all 值表示用户始终可以登录，空值（空白）意味着用户永远不能登录。用逗号分隔日期和时间，用分号分隔日期和时间单元（例如，M,4AM-5PM;T,1PM-3PM）。指定时间时不要使用空格
/usercomment:"text"	指定管理员添加或更改账户的“用户注释”为文本加上引号
/workstations:{ComputerName[,...] *}	最多列出 8 个用户可以登录到网络的工作站，多项之间用逗号分隔。如果/workstations 没有列表，或列表为星号*，则该用户可以从任何计算机登录

2.7.3 全局组管理——net group

如果要添加、显示或修改域中的全局组，并在组中添加用户账户，则使用 Net group 命令来实现。如果要为用户分配一定的权限，只要将用户账户添加到相应的组中即可。

1. 添加用户组

要添加一个用户组 coolpen，在命令提示符下输入如下命令：

```
net group coolpen /add
```

按回车键，该组被添加到域中，如图 2-46 所示。

要查看当前域中有哪些组，在命令提示符下输入如下命令：

```
net group
```

按回车键，显示当前域中所有的用户组，如图 2-47 所示，其中 coolpen 为刚添加的组。

2. 在组中添加用户账户

例如将用户 lhn 和 liuxh 添加到组 coolpen 中，在命令提示符下输入如下命令：

```
net group coolpen lhn liuxh /add
```

按回车键，用户 lhn 和 liuxh 即被添加到组 coolpen 中，如图 2-48 所示。

如果要查看组 coolpen 中的所有用户账户，在命令提示符下输入如下命令：

```
net group coolpen
```

按回车键，显示该组中的所有成员，如图 2-49 所示。

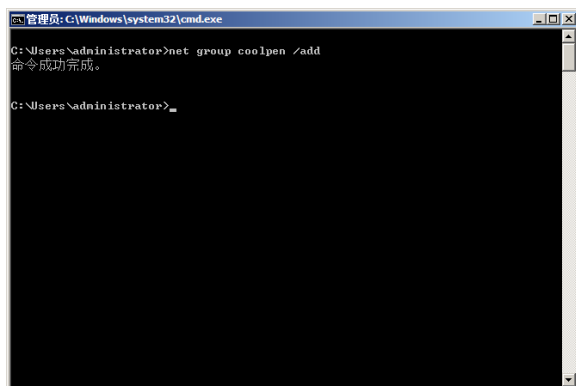


图 2-46 添加用户组

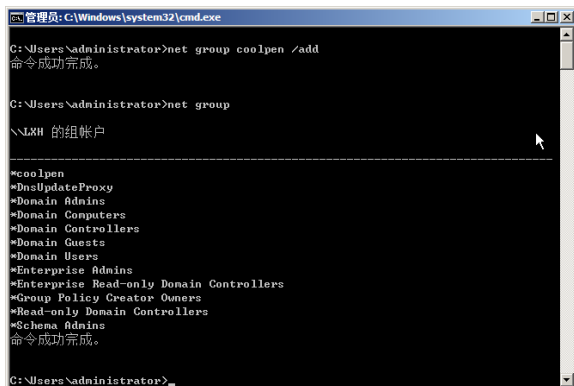


图 2-47 查看用户组

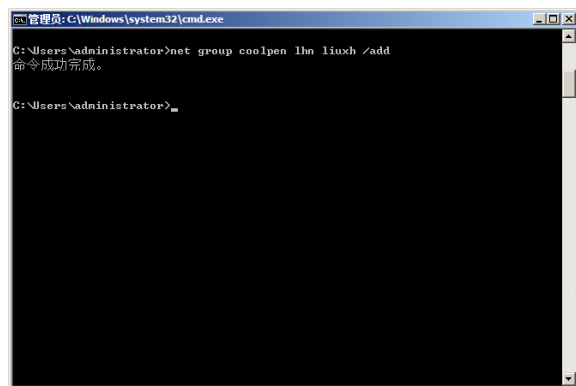


图 2-48 将用户添加到组

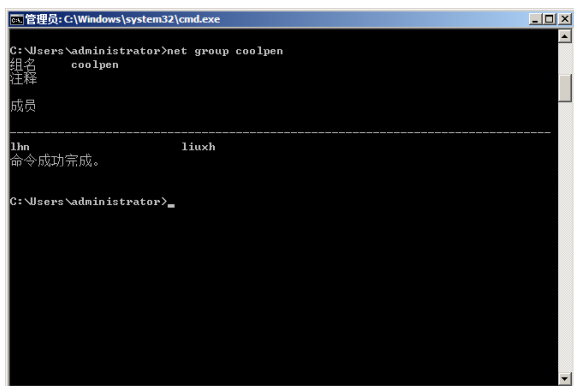


图 2-49 显示组中的所有成员

3. net group 命令说明

net group 命令的语法格式为：

```
net group [groupname [/comment:"text"]] [/domain]
net group groupname {/add [/comment:"text"] | /delete} [/domain]
net group groupname username [...] {/add | /delete} [/domain]
```

参数说明如下。

- (1) **groupname**：指定要添加、扩展或删除的组名称，仅指定组名则显示组中的用户列表。
- (2) **/comment:"text"**：为新建或已经存在的组添加注释，注释可以包含多达 48 个字符。
- (3) **/domain**：在当前域的主域控制器上执行操作，否则操作将在本地计算机上执行。
- (4) **/add**：添加组或在组中添加用户。
- (5) **/delete**：删除组或其中的用户。
- (6) **userName[...]**：列出要添加或删除的一个或多个用户名，多个用户名之间用空格分隔。



注意：

为组指定权限时，组中的每个成员都自动获得这些权限。在输出中，net group 将先输出包含带有星号 (*) 的用户和组的组。



2.7.4 本地组管理——net localgroup

net localgroup 用来添加、显示或修改本地组，并在本地组中添加用户。net localgroup 命令的使用方法与 net Group 命令类似，不同是 net Group 用来设置域组，而 net localgroup 则用来设置本地组。

1. 添加本地组

在计算机中添加本地组 book，在命令提示符下输入如下命令：

```
net localgroup book
```

按回车键，本地组 book 添加成功，如图 2-50 所示。

在命令提示符下输入如下命令：

```
net localgroup
```

按回车键，显示当前计算机中所有的本地组。其中 book 为刚刚添加的组，如图 2-51 所示。

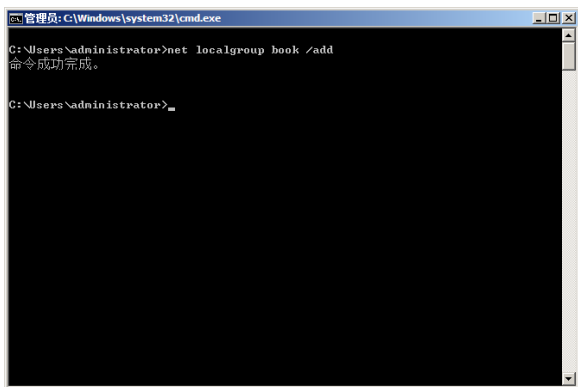


图 2-50 添加本地组

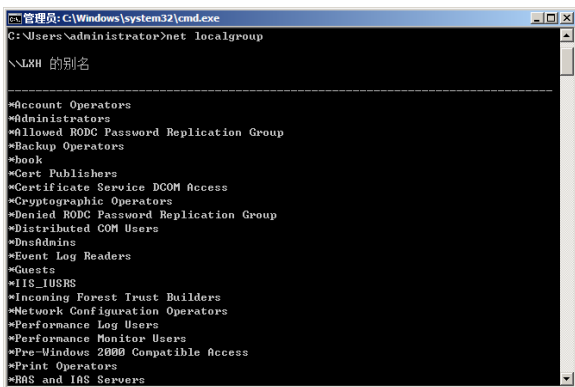


图 2-51 当前计算机中所有的本地组

2. 在本地组中添加用户

为将用户 lhn 添加到本地组 book 中，在命令提示符下输入如下命令：

```
net localgroup book lhn /add
```

按回车键，成功添加用户，如图 2-52 所示。

现在来查看用户组 book 中的用户，在命令提示符下输入如下命令：

```
net localgroup book
```

按回车键，显示 book 组中所有的成员，如图 2-53 所示。

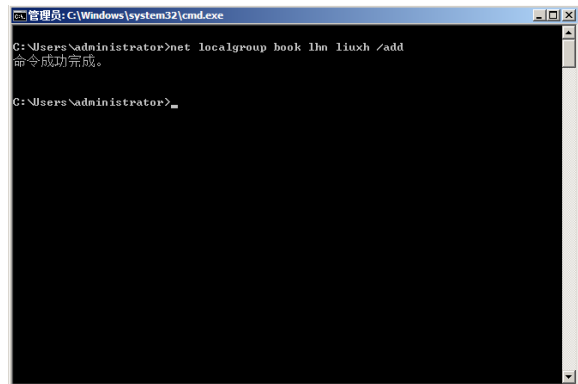


图 2-52 在本地组中添加用户

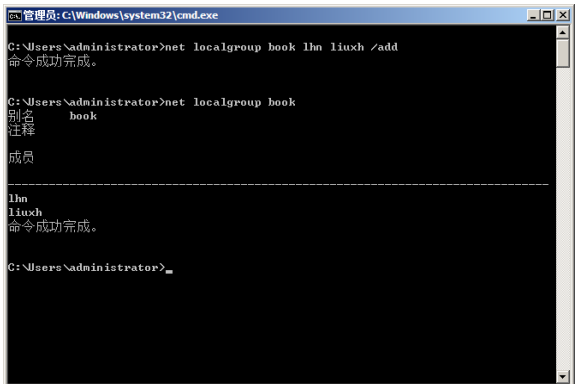


图 2-53 book 组中所有的成员

3. net localgroup 命令说明

net localgroup 的语法格式为：


```
net localgroup [GroupName [/comment:"text"]] [/domain]
net localgroup [GroupName {/add [/comment:"text"] | /delete} [/domain]]
net localgroup [GroupName name [ ...]{/add | /delete} [/domain]]
```

参数说明如下。

- (1) GroupName: 指定要添加、扩展或删除的本地组名称。
- (2) /comment:"text": 为新建或已经存在的组添加注释, 最多可以包含 48 个字符, 文本必须加上引号。
- (3) /domain: 在当前域的主域控制器执行操作, 否则操作将在本地计算机上执行。
- (4) name [...]: 列出一个或多个用户名或组名, 以添加或从本地组中删除。
- (5) /add: 在组中添加用户账户, 不过必须事先已创建相应的用户。
- (6) /delete: 从本地组中删除组或用户。

提示

如果运行 net localgroup 命令时不带任何参数, 则显示所有的本地组。

2.7.5 身份识别工具——whoami

whoami 命令可以获取本地系统中当前登录用户的用户名和组信息, 以及相应的安全标识符(SID)、特权和登录标识符(logon ID)。如果没有指定开关参数, 则用 NTLM 格式(域\用户名)显示用户名。

1. 显示当前所有信息

在命令提示符下输入如下命令:

```
whoami /all
```

按回车键, 显示用户名和安全标识符(SID)、组名、类型、属性及其 SID、特权及其状态(例如, 启用或禁用), 以及登录 ID 等信息, 如图 2-54 所示。

2. whoami 命令说明

whoami 命令的语法格式为:

```
whoami [/upn | /fqdn | /logonid]
whoami { [/user] [/groups] [/priv] } [/fo format] [/nh]
whoami /all [/FO nh] [/format]
```



图 2-54 当前所有信息

参数说明如下。

- (1) /logonid: 显示当前用户的登录 ID。

- (2) /upn: 使用用户主体 (User Principal) 格式显示用户名称 (UPN) 格式。
- (3) /fqdn: 用完全合格的 (Fully Qualified) 格式显示用户名可分辨名称 (FQDN) 格式。
- (4) /user: 显示当前用户的信息以及安全标识符 (SID)。
- (5) /groups: 显示当前用户的组成员信息、账户类型和安全标识符 (SID), 以及属性。
- (6) /priv: 显示当前用户的安全特权。
- (7) /all: 显示当前用户名、属于的组和安全标识符 (SID), 以及当前用户访问令牌的特权。
- (8) /fo format: 指定要显示的输出格式, 有效值为 TABLE、LIST 和 CSV。CSV 格式不显示列标题, 默认为 TABLE。
- (9) /nh: 指定在输出中不显示列标题, 只对 TABLE 和 CSV 格式有效。

2.8 AD DS 域服务管理命令

虽然 Server Core 中 Active Directory 域服务没有图形界面, 但所有的操作均可利用命令来完成, 如为域设置用户、组、计算机和组织单位等。

2.8.1 添加目录对象工具——dsadd

如果要在域中添加特定类型的对象, 包括计算机账户、用户、组、组织单元、服务器及分区等, 则利用 dsadd 命令。不过, 运行该命令的用户账户必须具备管理员权限。

dsadd 命令主要包括以下子命令。



注意:

在添加对象时必须保证待添加的对象尚未存在, 否则会出现错误。

1. dsadd computer——在域中添加计算机

例如在域 coolpen.net 的容器 computers 中添加计算机账户 hstjl, 在命令提示符下输入如下命令:

```
dsadd computer cn=hstjl,cn=computers,dc=coolpen,dc=net
```

按回车键, 添加计算机账户 hstjl 成功, 如图 2-55 所示。

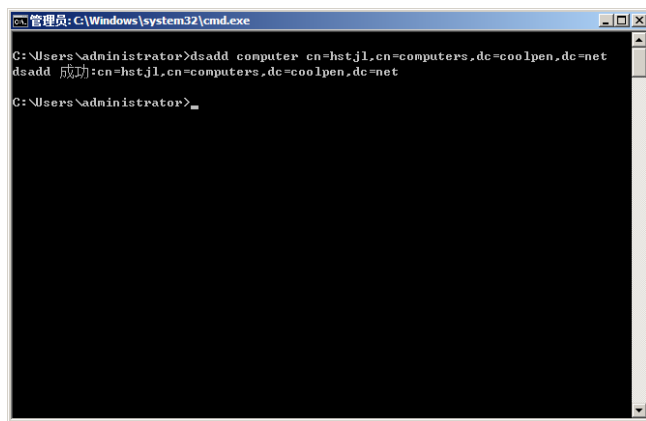


图 2-55 添加计算机账户 hstjl 成功

dsadd computer 的语法格式为:

```
dsadd computer <ComputerDN> [-samid <SAMName>] [-desc <Description>] [-loc <Location>]
[-memberof <Group ...>] [{-s <Server> | -d <Domain>}] [-u <UserName>] [-p {<Password> |
*}] [-q] [{-uc | -uco | -uci}]
```

参数说明如下。



(1) ComputerDN: 必需项, 指定要添加的计算机名称。如果目标对象被省略, 将从标准输入 (stdin) 中读取。

(2) -samid SAMName: 指定将 SAM 名称用做此计算机的唯一 SAM 账户名。如果未指定该参数, SAM 账户名会从 ComputerDN 中使用的公用名属性中导出。

(3) -desc: 设置要添加的计算机的描述。

(4) -loc: 设置要添加的计算机的位置。

(5) -memberof <Group ...>: 指定要计算机成为其成员的组。



注意:

如果提供的值包含空格, 需用引号将内容引起 (例如, "CN=DC 2,OU=DomainControllers,DC=Microsoft,DC=Com")。如果要为一个参数提供多个值, 则使用空格分隔。



2. dsadd contact——在域中添加联系人

例如在域 coolpen.net 中添加一个联系人 lxx, 其名为 "liuxiaohui", 电子邮件地址为 "hslxx@163.com", 在命令提示符下输入如下命令:

```
dsadd contact CN=coolpen,DC=coolpen,DC=net -display liuxiaohui -email hslxx@163.com
```

按回车键, 联系人添加成功, 如图 2-56 所示。

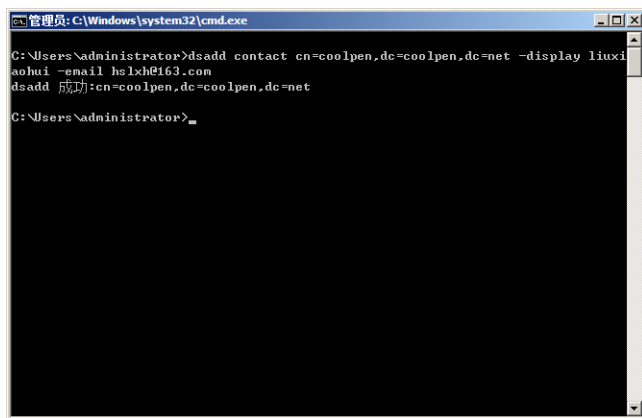


图 2-56 添加联系人成功

dsadd contact 命令语法格式为:

```
dsadd contact ContactDN [-fn FirstName] [-mi Initial] [-ln LastName] [-display DisplayName] [-desc Description] [-office Office] [-tel PhoneNumber] [-email Email] [-hometel HomePhoneNumber] [-pager PagerNumber] [-mobile CellPhoneNumber] [-fax FaxNumber] [-iptel IPPhoneNumber] [-title Title] [-dept Department] [-company Company] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]
```

参数说明如下。

(1) ContactDN: 必需项, 指定要添加的联系人可分辨名称。如果省略, 则将从标准输入 (stdin) 中获取该名称。

(2) -fn FirstName: 指定要添加的联系人名字。

(3) -mi Initial: 指定要添加的联系人中间名的首字母。

(4) -ln LastName: 指定要添加的联系人姓氏。

(5) -display DisplayName: 指定要添加的联系人显示名。

(6) -desc: 设置要添加的联系人描述。

- (7) -office: 指定要添加的联系人的办公室位置。
- (8) -tel PhoneNumbe: 指定要添加的联系人的电话号码。
- (9) -email: 指定要添加的联系人的电子邮件地址。
- (10) -hometel HomePhoneNumber: 指定要添加的联系人的家庭电话号码。
- (11) -pager PagerNumber: 指定要添加的联系人的寻呼机号码。
- (12) -mobile CellPhoneNumber: 指定要添加的联系人的移动电话号码。
- (13) -fax FaxNumber: 指定要添加的联系人的传真号码。
- (14) -iptel IPPhoneNumber: 指定要添加的联系人的 IP 电话号码。
- (15) -title: 指定要添加的联系人的称谓。
- (16) -dept: 指定要添加的联系人的部门。
- (17) -company: 指定要添加的联系人的公司信息。

3. dsadd group——在域中添加组

例如在域 coolpen.net 中添加一个组 book，在命令提示符下输入如下命令：

```
dsadd group "cn=book,dc=coolpen,dc=net"
```

按回车键，组 book 被添加到域中，如图 2-57 所示。

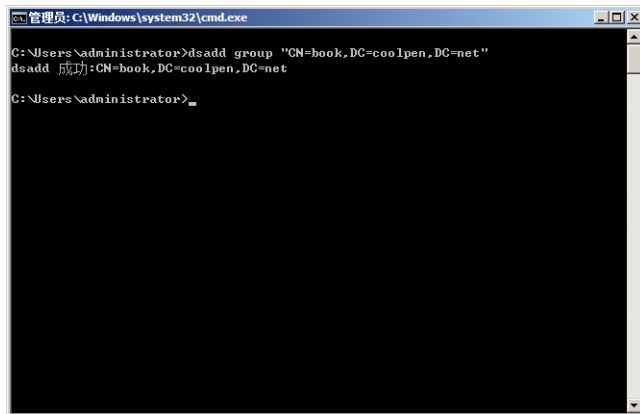


图 2-57 添加组 book

dsadd group 命令的语法格式为：

```
dsadd group <GroupDN> [-secgrp {yes | no}] [-scope {l | g | u}] [-samid <SAMName>]  
[-desc <Description>] [-memberof <Group ...>] [-members <Member ...>] [{-s <Server> | -d  
<Domain>}] [-u <UserName>] [-p {<Password> | *}] [-q] [{-uc | -uco | -uci}]
```

参数说明如下。

- (1) GroupDN: 必需项，指定要添加的组。
- (2) -secgrp {yes|no}: 指定要添加的组是安全组 (yes)，还是通信组 (no)，默认为安全组。
- (3) -scope {l|g|u}: 指定要添加的组的作用域是本地 (l)、全局 (g)，还是通用 (u)。如果域处于混合模式下，则不支持通用作用域。默认为全局。
- (4) -memberof: 指定此新组应添加至其中的组。
- (5) -members: 指定要添加到新组的成员。

4. dsadd ou——在域中添加组织单位

例如在域 coolpen.net 中添加一个名为“dianjiao”的组织单元，在命令提示符下输入如下命令：

```
dsadd ou "OU=dianjiao,DC=coolpen,DC=net" -desc "This is Dianjiao Shi"
```

按回车键，组织单位 dianjiao 被成功添加到域中，并且描述信息为“This is Dianjiao Shi”，如图 2-58 所示。

dsadd ou 命令的语法格式为:

```
dsadd ou OrganizationalUnitDN [-desc Description] [{-s Server | -d Domain}] [-u UserName]
[-p {Password | *}] [-q] [{-uc | -uco | -uci}]
```

其中的 OrganizationalUnitDN 参数为要添加的 OU 的名称, 其他参数的说明请参见前面所述内容, 此处不再重复。

5. dsadd user——在域中添加用户

例如在域中的组织单位 dianjiao 中添加一个用户 czc, 密码为 abcd_123, 公司为 aiyi, 部门为编辑部。在命令提示符下输入如下命令:

```
dsadd user "cn=czc,ou=dianjiao,dc=coolpen,dc=net" -company aiyi -dept 编辑部 -pwd
abcd_123
```

按回车键, 添加用户 czc 到域中, 如图 2-59 所示。

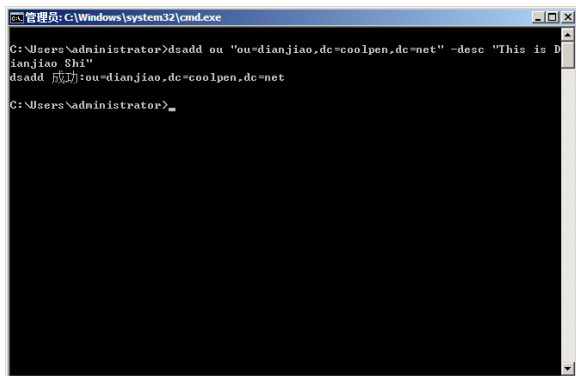


图 2-58 成功添加组织单位

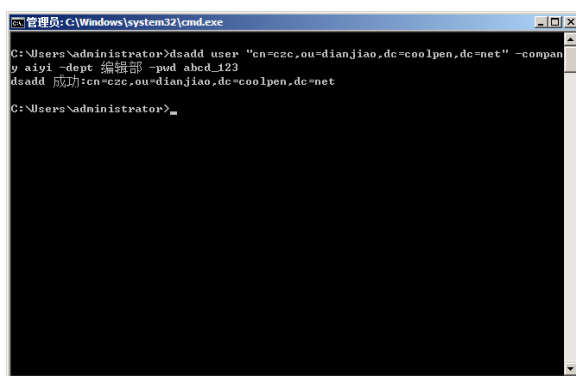


图 2-59 添加用户 czc

dsadd user 命令的语法格式为:

```
dsadd user <UserDN> [-samid <SAMName>] [-upn <UPN>] [-fn <FirstName>] [-mi <Initial>]
[-ln <LastName>] [-display <DisplayName>] [-empid <EmployeeID>] [-pwd {<Password> | *}]
[-desc <Description>] [-memberof <Group ...>] [-office <Office>] [-tel <Phone#>] [-email
<Email>] [-hometel <HomePhone#>] [-pager <Pager#>] [-mobile <CellPhone#>] [-fax <Fax#>]
[-iptel <IPPhone#>] [-webpg <WebPage>] [-title <Title>] [-dept <Department>] [-company
<Company>] [-mgr <Manager>] [-hmdir <HomeDir>] [-hmdrv <DriveLtr:>] [-profile
<ProfilePath>] [-loscr <ScriptPath>] [-mustchpwd {yes | no}] [-canchpwd {yes | no}]
[-reversiblepwd {yes | no}] [-pwdneverexpires {yes | no}] [-acctexpires <NumDays>]
[-disabled {yes | no}] [{-s <Server> | -d <Domain>}] [-u <UserName>] [-p {<Password> |
*}] [-q] [{-uc | -uco | -uci}]
```

参数说明如下。

- (1) <UserDN>: 必需项, 指定要添加的用户名称。
- (2) -upn UPN: 设置用户主体名称。
- (3) -fn FirstName: 设置用户名。
- (4) -mi Initial: 设置用户中间名的首字母。
- (5) -ln LastName: 设置用户姓氏。
- (6) -display DisplayName: 设置用户的显示名。
- (7) -empid EmployeeID: 设置用户的雇员 ID。
- (8) -pwd {<Password> | *}: 设置用户密码, 如果设置为 *, 则提示输入密码。
- (9) -desc <Description>: 设置用户的描述。
- (10) -memberof <Group ...>: 设置用户要加入的组。
- (11) -office <Office>: 设置用户的办公室位置。

- (12) `-tel <Phone#>`: 设置用户的电话号码。
- (13) `-email <Email>`: 设置用户的电子邮件地址。
- (14) `-hometel <HomePhone#>`: 设置用户的家庭电话号码。
- (15) `-pager <Pager#>`: 设置用户的寻呼机号码。
- (16) `-mobile <CellPhone#>`: 设置用户的移动电话号码。
- (17) `-fax <Fax#>`: 设置用户的传真号码。
- (18) `-iptel <IPPhone#>`: 设置用户的 IP 电话号码。
- (19) `-webpg <WebPage>`: 设置用户 Web 页的 URL。
- (20) `-title <Title>`: 设置用户的职务。
- (21) `-dept <Department>`: 设置用户的部门。
- (22) `-company <Company>`: 设置用户的公司信息。
- (23) `-mgr <Manager>`: 设置用户的经理。
- (24) `-hmdir <HomeDir>`: 设置用户主的主目录位置,如果是通用命名约定(UNC)路径,必须使用 `-hmdrv` 参数指定要映射到此路径的驱动器号。
- (25) `-hmdrv <DriveLtr>`: 设置用户主驱动器号(例如, E:)。
- (26) `-profile <ProfilePath>`: 设置用户的配置文件路径。
- (27) `-loscr <ScriptPath>`: 设置用户的登录脚本路径。
- (28) `-mustchpwd {yes | no}`: 设置用户在下次登录时是否更改密码,默认为不更改(no)。
- (29) `-canchpwd {yes | no}`: 用户是否可以更改密码(yes 为可以更改, no 为不能更改)。默认为 yes。如果 `-mustchpwd` 的参数值为 yes, 则该参数值必须也为 yes。
- (30) `-reversiblepwd {yes | no}`: 是否使用可逆加密保存密码,默认值为不能使用可逆加密(no)。
- (31) `-pwdneverexpires {yes | no}`: 密码是否永远不过期,默认为过期(no)。
- (32) `-acctexpires <NumDays>`: 设置用户账户从今天起在<NumDays>天内过期,0 值表示今天结束后账户就过期;正值表示账户在未来过期;负值表示将以前的时间设置为到期时间;字符串值“never”表示账户永不过期。
- (33) `-disabled {yes | no}`: 设置是否禁用该用户账户,默认为不禁用(no)。

►► 2.8.2 修改目录对象——dsmod

`dsmod` 命令用来修改目录中特定类型的现有对象,包括计算机账户、用户、组、组织单元、服务器、分区及磁盘配额等,该命令包括以下子命令。

1. `dsmod computer`——修改域中的计算机

`dsmod computer` 命令用来修改域中现有计算机的属性,例如禁用、启用及复位计算机账户等,并可同时操作多个计算机账户。

例如,要禁用域 `coolpen.net` 中的计算机账户 `hslhn`,在命令提示符下输入如下命令:

```
dsmod computer cn=hslhn,cn=computers,dc=coolpen,dc=net -disabled yes
```

按回车键,禁用计算机账号,如图 2-60 所示。

如果要同时禁用多个计算机账户,如 `tjl` 及 `czc`,在命令提示符下输入如下命令:

```
dsmod computer "cn=tjl,cn=computers,dc=coolpen,dc=net" "cn=czc,cn=computers,dc=coolpen,dc=net" -disabled yes
```

按回车键,禁用多个计算机账户,如图 2-61 所示。

如果要复位计算机账户,如 `lhn`,在命令提示符下输入如下命令:

```
dsmod computer "cn=lhn,cn=computers,dc=coolpen,dc=net" -reset
```

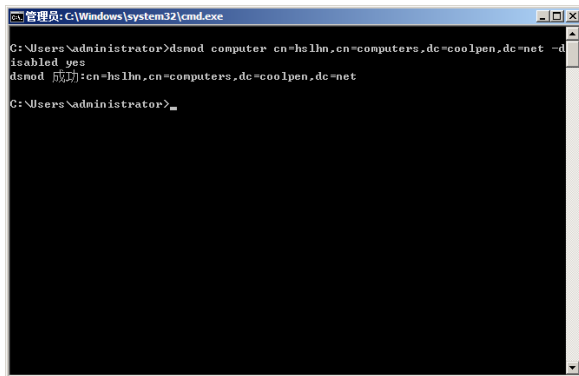



图 2-60 禁用计算机账户

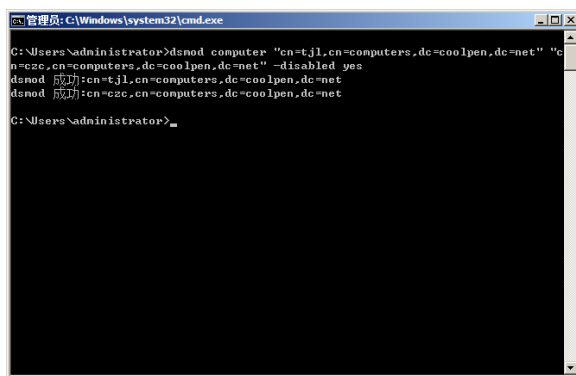


图 2-61 同时禁用多个计算机账户

按回车键，成功禁用计算机账户 lhn，如图 2-62 所示。

dsmod computer 命令的语法格式为：

```
dsmod computer <ComputerDN ...> [-desc <Description>] [-loc <Location>] [-disabled {yes | no}] [-reset] [{-s <Server> | -d <Domain>}] [-u <UserName>] [-p {<Password> | *}] [-c] [-q] [{-uc | -uco | -uci}]
```

参数说明如下。

- (1) <ComputerDN ...>: 指定要修改的一个或多个计算机账户的可分辨名称 (DN)。
- (2) -desc <Description>: 指定对要修改计算机账户的描述。
- (3) -loc <Location>: 指定要修改的计算机对象的位置。
- (4) -disabled {yes | no}: 指定是否禁止该计算机账户登录 (yes 为禁止登录，no 为允许)。
- (5) -reset: 重置计算机账户。

其他参数介绍请参见前面所述内容，此处不再赘述。

2. dsmod contact——修改域中的联系人

dsmod contact 命令用来修改域中一个或多个现有联系人的属性，包括电话、传真及电子邮件等。

例如要将用户账户 lxx 的职务修改为主任，电子邮件修改为 lxx@coolpen.net，在命令提示符下输入如下命令：

```
dsmod contact cn=lxx,dc=coolpen,dc=net -title 主任 -email lxx@coolpen.net
```

按回车键，用户的职务和电子邮件被成功更改，如图 2-63 所示。

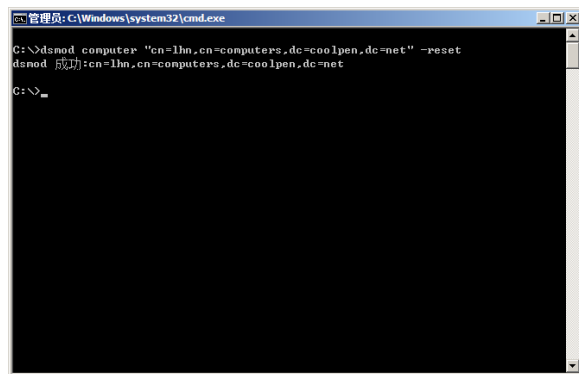


图 2-62 成功禁用计算机账户

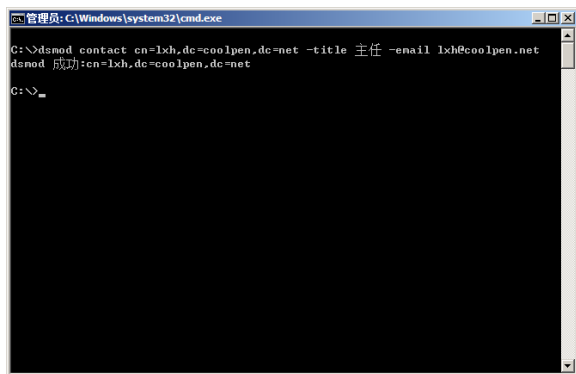


图 2-63 修改联系人的职务和电子邮件

Dsmod contact 命令的语法格式为：

```
dsmod contact <ContactDN ...> [-fn <FirstName>] [-mi <Initial>] [-ln <LastName>] [-display <DisplayName>] [-desc <Description>] [-office <Office>] [-tel <Phone#>] [-email <Email>] [-hometel <HomePhone#>] [-pager <Pager#>] [-mobile <CellPhone#>] [-fax <Fax#>]
```

```
[-iptel <IPPhone#>] [-title <Title>] [-dept <Department>] [-company <Company>] [{-s  
<Server> | -d <Domain>}] [-u <UserName>] [-p {<Password> | *}] [-c] [-q] [{-uc | -uco |  
-uci}]
```

参数说明如下。

- (1) <ContactDN ...>: 必需项, 指定要修改联系人的可分辨名称 (DN)。
- (2) -fn FirstName: 指定要修改联系人名字。
- (3) -mi Initial: 指定要修改联系人中间名的首字母。
- (4) -ln LastName: 指定要修改联系人的姓。
- (5) -display DisplayName: 指定要修改的联系人的显示名称。
- (6) -desc Description: 指定对要修改联系人的描述。
- (7) -office Office: 指定要修改联系人的办公地点。
- (8) -tel PhoneNumber: 指定要修改联系人的电话号码。
- (9) -email Email: 指定要修改联系人的电子邮件地址。
- (10) -hometel CellPhoneNumber: 指定要修改联系人的家庭电话号码。
- (11) -pager PagerNumber: 指定要修改联系人的寻呼机号码。
- (12) -mobile CellPhoneNumber: 指定要修改联系人的移动电话号码。
- (13) -fax FaxNumber: 指定要修改联系人的传真号码。
- (14) -iptel IPPhoneNumber: 指定要修改联系人的 IP 电话号码。
- (15) -title Title: 指定要修改联系人的职务。
- (16) -dept Department: 指定要修改联系人的部门。
- (17) -company Company: 指定要修改联系人的公司信息。

其他参数的介绍请参见前面所述内容, 此处不再赘述。

3. dsmod group——修改域中的组

dsmod group 命令用来修改域中一个或多个现有组的属性, 例如在组中添加或删除用户及转换组类型等。

如果要将用户 czc 和 lhn 添加到域 coolpen.net 的组 book 中, 在命令提示符下输入如下命令:

```
dsmod group "cn=book,dc=coolpen,dc=net" -addmbr "cn=czc,cn=users,dc=coolpen,dc=net"  
"cn=lhn,cn=users,dc=coolpen,dc=net"
```

按回车键, 用户 czc 和 lhn 添加到 book 组中, 如图 2-64 所示。

如果要从现有的组 book 中删除用户 lhn, 在命令提示符下输入如下命令:

```
dsmod group "cn=book,dc=coolpen,dc=net" -rmmbr "cn=lhn,cn=users,dc=coolpen,dc=net"
```

按回车键, 用户 lhn 被从组 book 中删除, 如图 2-65 所示。

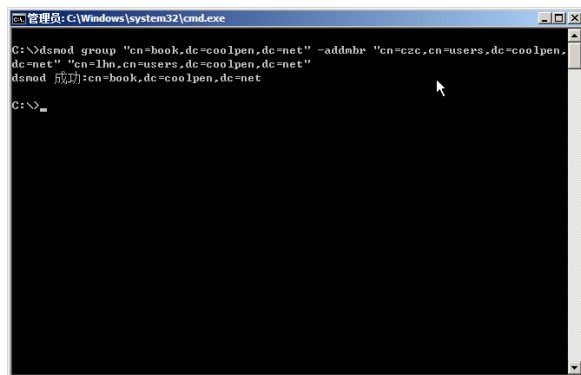


图 2-64 添加两个用户到组

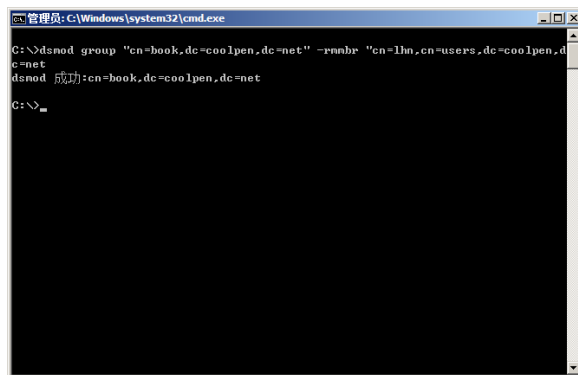


图 2-65 从组中删除用户

dsmod group 也可以转换组的类型，例如，将组 book 的类型从安全组转换为非安全组，在命令提示符下输入如下命令：

```
dsmod group "cn=book,dc=coolpen,dc=net" -secgrp no
```

按回车键，book 组转换为非安全组，如图 2-66 所示。

dsmod group 的语法格式为：

```
dsmod group <GroupDN ...> [-samid <SAMName>] [-desc <Description>] [-secgrp {yes | no}] [-scope {l | g | u}] [{-addmbr | -rmmbr | -chmbr} <Member ...>] [{-s <Server> | -d <Domain>}] [-u <UserName>] [-p {<Password> | *}] [-c] [-q] [{-uc | -uco | -uci}]
```

参数说明如下。

- (1) <GroupDN ...>：必需项，设置要修改组的可分辨名称（DN）。
 - (2) -samid <SAMName>：设置要修改组的 SAM 账户名。
 - (3) -desc <Description>：设置要修改组的描述。
 - (4) -secgrp {yes | no}：将组类型设置为安全组（yes）或通信组（no）。
 - (5) -scope {l | g | u}：将组作用域设置为本地、全局或通用。如果域处于混合模式，则不支持通用作用域。同时，不可能将本地域组转换为全局组；反之亦然。
 - (6) {-addmbr | -rmmbr | -chmbr} <Member ...>：从组中添加、删除 GroupDN 指定的成员，或替代 <MemberDN ...>指定的成员，成员列表必须跟随在 -addmbr、-rmmbr 和 -chmbr 参数之后。
- 其他参数的介绍请参见前面所述内容，此处不再重复。

4. dsmod ou——修改域中的组织单位

dsmod ou 命令用来修改目录中一个或多个现有组织单位的属性，主要是描述信息。

例如，要更改组织单位 dianjiao 的描述，可在命令提示符下输入如下命令：

```
dsmod ou "ou=dianjiao,dc=coolpen,dc=net" -desc "Welcome to Dianjiao"
```

按回车键，命令成功执行。更改组织单位的描述，如图 2-67 所示。

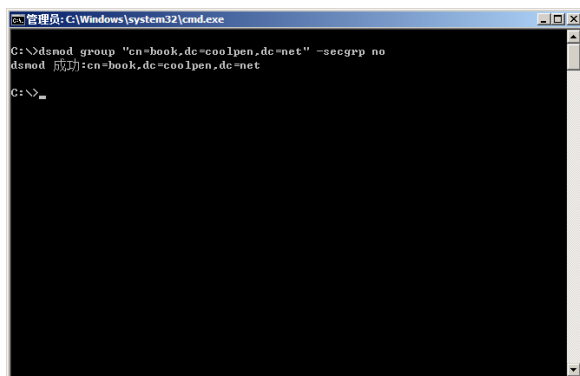


图 2-66 转换组类型

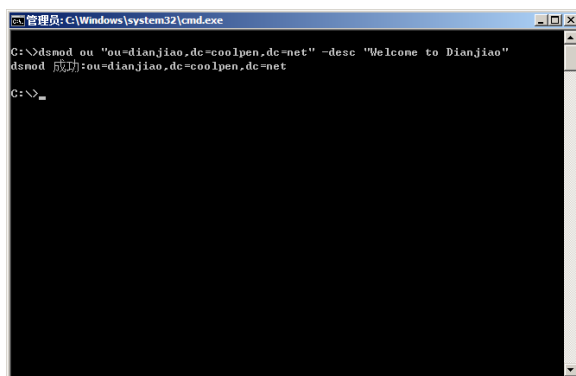


图 2-67 更改组织单位的描述

dsmod ou 命令的语法格式为：

```
dsmod ou <OrganizationalUnitDN ...> [-desc <Description>] [{-s <Server> | -d <Domain>}] [-u <UserName>] [-p {<Password> | *}] [-c] [-q] [{-uc | -uco | -uci}]
```

参数说明如下。

- (1) <OrganizationalUnitDN ...>：必需项，指定要修改的组织单位的可分辨名称（DN）。
- (2) -desc Description：指定要修改的组织单位的描述。

其他参数的介绍请参见前面所述内容，此处不再重复。

5. dsmod server——修改域控制器属性

dsmod server 命令用来修改域控制器的属性。

例如，要将域控制器 lxx 启用为全局编录服务器，在命令提示符下输入如下命令：

```
dsmod server "CN=lxx,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=coolpen,DC=net" -isgc yes
```

按回车键，命令成功执行，域控制器 lxx 被成功启用为全局编录服务器，如图 2-68 所示。

提示

服务器的实际的名称为：

Coolpen.net/Configuration/Sites/Default-First-Site-Name/Servers/LXX/NTDS Settings。

则命令行格式为：

CN=lxx,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=coolpen,DC=net

dsmod server 的语法格式为：

```
dsmod server <ServerDN ...> [-desc <Description>] [-isgc {yes | no}] [{-s <Server> | -d <Domain>}] [-u <UserName>] [-p {<Password> | *}] [-c] [-q] [{-uc | -uco | -uci}]
```

参数说明如下。

- (1) <ServerDN ...>：必需项，指定要修改的一个或多个服务器的可分辨名称。
- (2) -desc <Description>：指定对要修改服务器的描述。
- (3) -isgc {yes | no}：设置为全局编录服务器（yes）或禁用此服务器（no）。

dsmod server 命令其他参数的介绍请参见前面所述内容，此处不再重复。

6. dsmod user——修改域中的用户

dsmod user 命令用来修改域中一个或多个用户的属性，如禁止和启用用户账户，以及更改用户密码等。

例如禁用用户 lxx，在命令提示符下输入如下命令：

```
dsmod user cn=lxh,cn=users,dc=coolpen,dc=net -disabled yes
```

按回车键，用户 lxx 被禁用，如图 2-69 所示。

如果要重新启用该用户，可运行如下命令：

```
dsmod user cn=lxh,cn=users,dc=coolpen,dc=net -disabled no
```

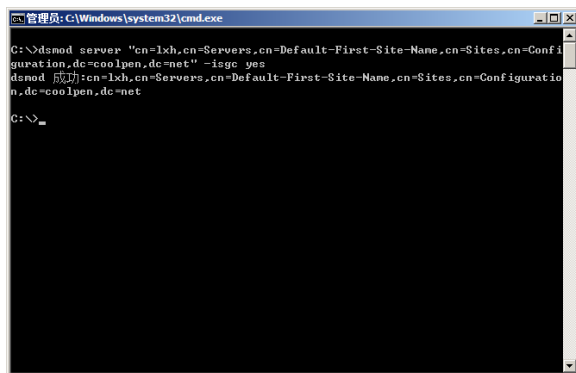


图 2-68 启用域控制器 lxx 为全局编录服务器

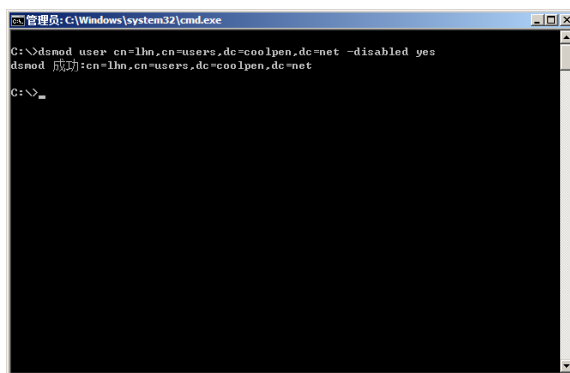


图 2-69 禁用用户

例如同时禁用多个账户 tj1、czc 和 liuxh，在命令提示符下输入如下命令：

```
dsmod user "cn=tj1,dc=coolpen,dc=net" "cn=czc,dc=coolpen,dc=net" "cn=liuxh,dc=coolpen,dc=net" -disabled yes
```

按回车键，多个用户账户被禁用，如图 2-70 所示。

例如更改用户 lhn 的密码为 ning_123，在命令提示符下输入如下命令：

```
dsmod user "cn=lhn,cn=users,dc=coolpen,dc=net" -pwd ning_123 -mustchpwd yes
```

按回车键，用户密码被成功更改，如图 2-71 所示。

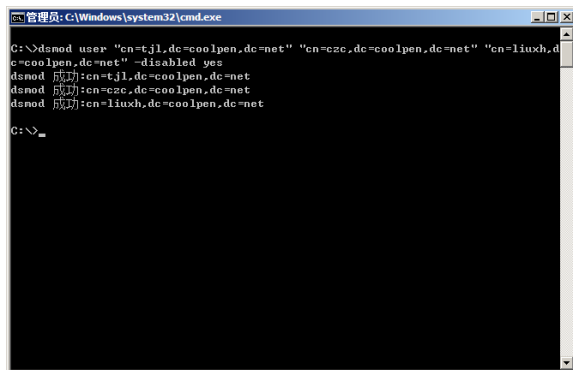


图 2-70 同时禁用多个账户

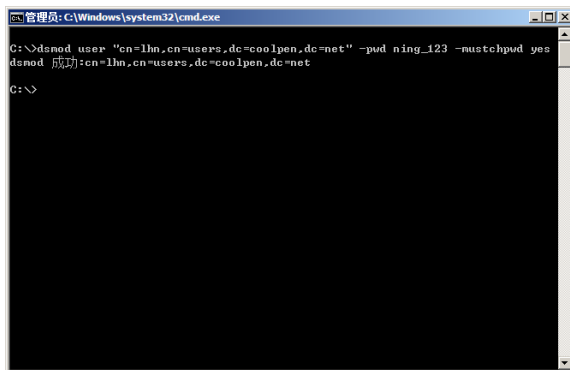


图 2-71 更改用户密码

提示

不能使用简单密码，必须为用户设置强密码。

dsmod user 命令的语法格式为：

```
dsmod user <UserDN ...> [-upn <UPN>] [-fn <FirstName>] [-mi <Initial>] [-ln <LastName>]
[-display <DisplayName>] [-empid <EmployeeID>] [-pwd {<Password> | *}] [-desc
<Description>] [-office <Office>] [-tel <Phone#>] [-email <Email>] [-hometel <HomePhone#>]
[-pager <Pager#>] [-mobile <CellPhone#>] [-fax <Fax#>] [-iptel <IPPhone#>] [-webpg
<WebPage>] [-title <Title>] [-dept <Department>] [-company <Company>] [-mgr <Manager>]
[-hmdir <HomeDir>] [-hmdrv <DriveLtr>:] [-profile <ProfilePath>] [-loscr <ScriptPath>]
[-mustchpwd {yes | no}] [-canchpwd {yes | no}] [-reversiblepwd {yes | no}] [-pwdneverexpires
{yes | no}] [-acctexpires <NumDays>] [-disabled {yes | no}] [{-s <Server> | -d <Domain>}]
[-u <UserName>] [-p {<Password> | *}] [-c] [-q] [{-uc | -uco | -uci}]
```

参数说明如下。

- (1) <UserDN ...>：必需项，设置要修改的用户的可分辨名称。
- (2) -upn <UPN>：设置要修改的用户对象的用户主体名称。
- (3) -fn <FirstName>：设置要修改的用户对象名。
- (4) -mi <Initial>：设置要修改的用户对象中间名的首字母。
- (5) -ln <LastName>：设置要修改的用户对象的姓。
- (6) -display <DisplayName>：设置要修改的用户对象的显示名称。
- (7) -empid <EmployeeID>：设置要修改的用户对象的雇员 ID。
- (8) -office <Office>：设置要修改的用户对象的办公地点。
- (9) -tel <Phone#>：设置要修改的用户对象的电话号码。
- (10) -email <Email>：设置要修改的用户对象的电子邮件地址。
- (11) -hometel <HomePhone#>：设置要修改的用户对象的家庭电话号码。
- (12) -pager <Pager#>：设置要修改的用户对象的寻呼机号码。
- (13) -mobile <CellPhone#>：设置要修改的用户对象的移动电话号码。
- (14) -fax <Fax#>：设置要修改的用户对象的传真号码。
- (15) -iptel <IPPhone#>：设置要修改的用户对象的 IP 电话号码。
- (16) -webpg <WebPage>：设置要修改的用户对象的网页 URL。

- (17) `-title <Title>`: 设置要修改的用户对象的职务。
- (18) `-dept <Department>`: 设置要修改的用户对象的部门。
- (19) `-company <Company>`: 设置要修改的用户对象的公司信息。
- (20) `-mgr <Manager>`: 设置要修改用户对象经理的可分辨名称。
- (21) `-hmdir <HomeDir>`: 设置要修改的用户对象的主目录位置, 如果 HomeDir 以 UNC 名称的形式给出, 则必须使用 `-hmdrv` 参数为此路径指定一个映射驱动器。
- (22) `-hmdrv <DriveLtr>`: 设置要修改的用户对象的主目录驱动器号 (例如 E:)。
- (23) `-profile <ProfilePath>`: 设置要修改的用户对象的配置文件路径。
- (24) `-loscr <ScriptPath>`: 设置要修改的用户对象的登录脚本路径。
- (25) `-mustchpwd {yes | no}`: 设置用户是否必须在下次登录时更改其密码 (yes 为必须更改, no 不必更改)。
- (26) `-canchpwd {yes | no}`: 设置用户是否可以更改其密码 (yes 为可以更改, no 为根本不能更改)。如果 `-mustchpwd` 的参数值为 yes, 则该参数值必须为 yes。
- (27) `-reversiblepwd {yes | no}`: 设置是否使用可逆加密方法存储用户密码 (yes 为使用, no 为不使用)。
- (28) `-pwdneverexpires {yes | no}`: 设置用户账户是否永不过期 (yes 为永不过期, no 为有时间限制)。
- (29) `-acctexpires <NumberDays>`: 设置从今天开始用户账户将过期的天数, 0 表示将今天的结束时间设置为到期时间, 正值表示将将来的时间设置为到期时间; 负值表示将以前的时间设置为到期时间。值 `never` 表示将该账户设置为永不过期, 例如, 0 表示该账户在今天结束时过期, -5 表示该账户 5 天前就已经到期, 5 表示该账户将在 5 天后到期。
- (30) `-disabled {yes | no}`: 指定是否禁止该用户账户登录 (yes 为禁止登录, no 为允许登录)。



注意:

在参数 `-webpg`、`-profile`、`-hmdir` 和 `-email` 中可以用特殊标记 `$username$` (区分大小写) 替换 SAM 账户名。例如, 如果该账户名是 “Denise”, 则可以使用 `-hmdir\users\Denise\home` 或 `-hmdir\users$username$\home` 的格式书写 `-hmdir` 位置参数。



2.8.3 删除目录对象——dsrm

`dsrm` 命令用来从目录中删除某种特定类型的对象或任何常规对象, 包括计算机账户、用户、组、组织单元、服务器、分区、子网、站点及配额等目录对象。

例如删除组织单位 `dianjiao` 及其中的所有对象, 在命令提示符下输入如下命令:

```
dsrm -subtree -noprompt -c OU=dianjiao,DC=coolpen,DC=net
```

按回车键, 组织单位 `dianjiao` 及其对象均被删除, 如图 2-72 所示。

例如删除组织单位 `hsnc` 下的用户 `liuxh`, 在命令提示符下输入如下命令:

```
dsrm -noprompt -c CN=liuxh,OU=hsnc,DC=coolpen,DC=net
```

按回车键, 组织单位 `hsnc` 下的用户 `liuxh` 被删除, 如图 2-73 所示。

例如删除组织单位 `hsnc` 中的所有对象, 但保留该组织单位, 在命令提示符下输入如下命令:

```
dsrm -subtree -exclude -noprompt -c "OU=hsnc,DC=coolpen,DC=net"
```

按回车键, 组织单位中的所有对象均被删除, 如图 2-74 所示。

`dsrm` 命令的语法格式为:

```
dsrm <ObjectDN ...> [-noprompt] [-subtree [-exclude]] [{-s <Server> | -d <Domain>}] [-u <UserName>] [-p {<Password> | *}] [-c] [-q] [{-uc | -uco | -uci}]
```

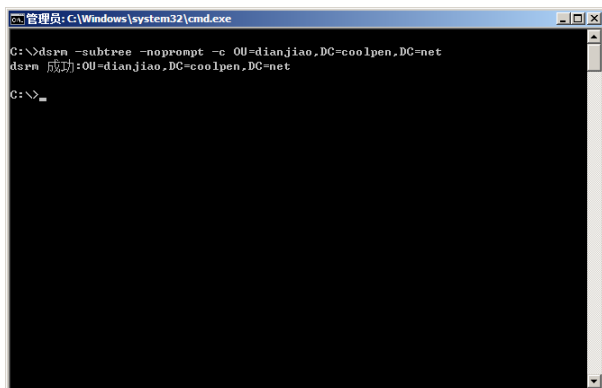



图 2-72 删除组织单位及其对象

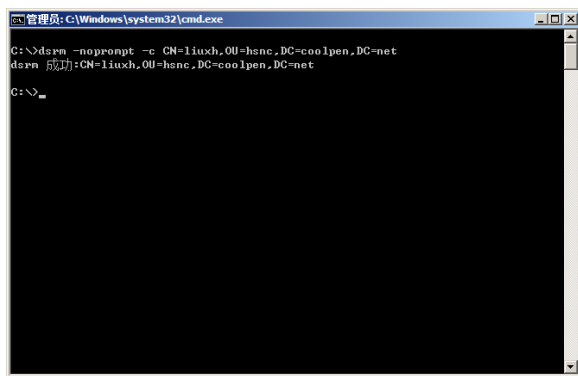


图 2-73 删除组织单位中的用户

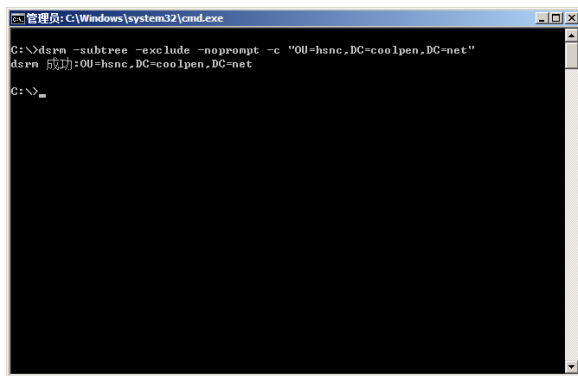


图 2-74 删除组织单位中的所有对象

参数说明如下。

- (1) <ObjectDN ...>: 必需项, 指定要删除对象的可分辨名称。
- (2) -noprompt: 设置可选的静态模式, 该模式在删除每个对象时不提示用户确认。默认情况下, 系统提示确认每一项删除操作。
- (3) -subtree [-exclude]: 指定应删除该对象及其下子树中包含的所有对象。
- (4) -exclude: 只能与-subtree 参数一同指定, 表明删除由 ObjectDN 给定的基础对象之下的子树时不应删除该对象。默认为只删除指定的基础对象。

DSRM 命令其他参数的说明请参见前面所述内容, 此处不再重复。

2.8.4 查询活动目录——dsquery

dsquery 命令可以查询域中所有存在的对象, 包括计算机账户、用户、组、组织单元、服务器、分区及站点等。

dsquery 包括以下子命令。

1. dsquery computer——查找计算机

例如在当前域中查找所有名称以“hs”开头的计算机, 并显示其可分辨的名称, 在命令提示符下输入如下命令:

```
dsquery computer domainroot -name hs*
```

按回车键, 列出所有以名称“hs”开头的计算机, 如图 2-75 所示。

例如查找容器 CN=Computers,dc=coolpen,DC=net 中所有的计算机账户, 在命令提示符下输入如下命令:

```
dsquery computer CN=Computers,dc=coolpen,DC=net
```

按回车键，显示容器“Computers”中所有的计算机账户，如图 2-76 所示。

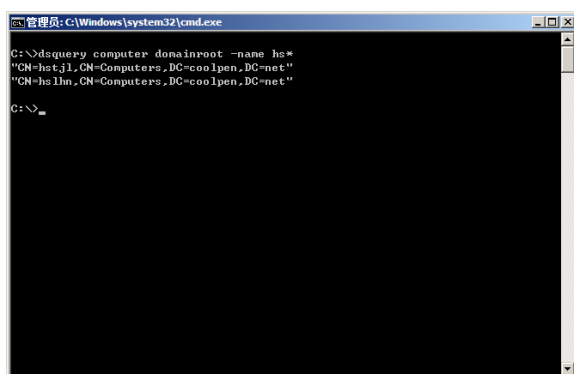


图 2-75 查找计算机

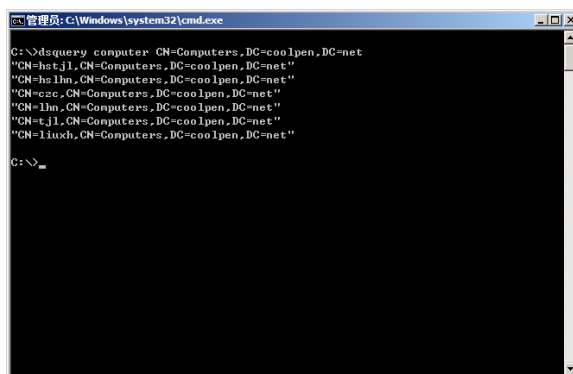


图 2-76 所有的计算机名称

dsquery computer 命令的语法格式为：

```
dsquery computer [{StartNode| forestroot | domainroot}] [-o {dn | rdn | samid}] [-scope {subtree | onelevel | base}] [-name Name] [-desc Description] [-samid SAMName] [-inactive NumberOfWeeks] [-stalepwd NumberOfDays] [-disabled] [{-s Server| -d Domain}] [-u UserName] [-p {Password|*}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

参数说明如下。

(1) {StartNode| forestroot | domainroot}：指定开始搜索的节点，可以指定林根目录（forestroot）、域根目录（domainroot）或节点的可分辨名称（StartNode）。如果指定 forestroot，则使用全局编录完成搜索。默认为 domainroot。

(2) -o {dn | rdn | samid}：指定搜索条目列表的显示格式，dn 显示每个条目的可分辨名称，rdn 显示每个条目的相对可分辨名称，samid 显示每个条目的 SAM 账户名。默认为 dn 格式。

(3) -scope {subtree | onelevel | base}：指定搜索范围，subtree 表示搜索范围是开始节点上的一个子树，onelevel 表示仅开始节点的直接子项。base 表示由开始节点代表的单一对象。如果将 forestroot 指定为 StartNode，则子树是唯一的有效范围。默认为 subtree。

(4) -name Name：搜索与 Name 相匹配的计算机。

(5) -desc Description：搜索描述属性与 Description 相匹配的计算机。

(6) -samid SAMName：搜索其 SAM 账户名与 SAMName 相匹配的计算机。

(7) -inactive NumberOfWeeks：搜索在指定周数内处于非活动状态（陈旧的）的全部计算机。

(8) -stalepwd NumberOfDays：搜索在指定天数内未更改密码的全部计算机。

(9) -disabled：搜索被禁用账户的全部计算机。

(10) {-s Server | -d Domain}：连接到指定远程服务器或域，默认情况下，计算机与登录域中的域控制器相连接。

(11) -u UserName：指定登录远程服务器的用户名，默认为已登录的用户。用户名可以是用户名、域\用户名或用户主体名称（UPN）。

(12) -p {Password|*}：指定登录到远程服务器的密码。如果输入*，则提示输入密码。

(13) -q：安静模式，不显示任何输出信息。

(14) -r：指定搜索期间搜索将使用递归或跟踪参照，默认在搜索期间搜索将不跟踪参照。

(15) -gc：指定搜索使用 Active Directory 全局编录。

(16) -limit NumberOfObjects：指定将返回与给定条件匹配的对象个数。如果 NumberOfObjects 的值为 0，则返回所有匹配的对象；如果未指定该参数，则默认显示前 100 条结果。

(17) {-uc | -uco | -uci}：-uc 指定从管道的输入或至管道输出使用 Unicode 格式；-uco 指定至管道或文件的输出使用 Unicode 格式；-uci 指定从管道或文件的输入使用 Unicode 格式。

2. dsquery contact——查找联系人

dsquery contact 命令用来查找域中的联系人。

例如要查看域 coolpen.net 的组织单位 coolpen 中所有的联系人信息，在命令提示符下键入如下命令：

```
dsquery contact OU=coolpen,DC=coolpen,DC=net
```

按回车键，命令成功执行，显示组织单位 coolpen 中的所有联系人，如图 2-77 所示。

dsquery contact 的语法格式为：

```
dsquery contact [{StartNode| forestroot | domainroot}] [-o {dn | rdn}] [-scope {subtree | onelevel | base}] [-name Name] [-desc Description] [{-s Server| -d Domain}] [-u UserName] [-p {Password| *}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

参数说明如下。

- (1) -name Name: 搜索联系人，Name 表示联系人的名称。
- (2) -desc Description: 搜索其描述属性与 Description 相匹配的联系人。
- (3) {-s Server| -d Domain}: 连接到指定远程服务器或域，默认情况下，计算机与登录域中的域控制器相连接。

其他参数请参阅前面所述内容，此处不再重复。

3. dsquery group——显示域中的组

dsquery group 命令用来在域中查找并显示组，Dsquery *则可显示域所有的组。

例如在当前域中查找所有名称以“hs”开头，并且描述以“衡水”开头的组，在命令提示符下输入如下命令：

```
dsquery group domainroot -name admin* -desc 衡水*
```

按回车键，列出域中所有符合条件的组，如图 2-78 所示。

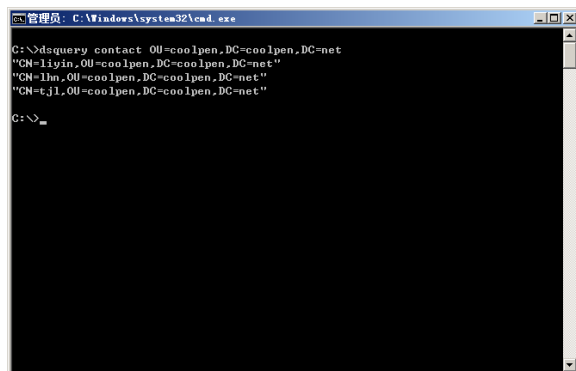


图 2-77 组织单位 coolpen 中的所有联系人

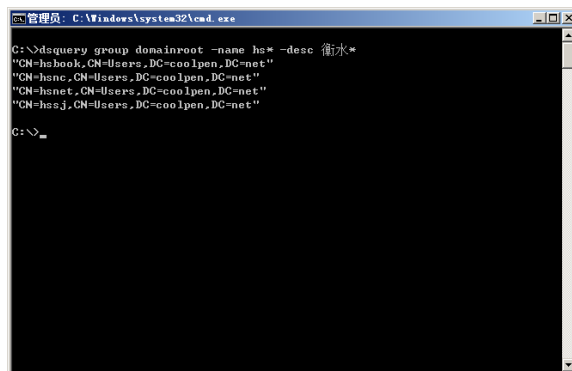


图 2-78 域中所有符合条件的组

例如在域 DC=coolpen,DC=net 中查找所有组，并显示其可分辨的名称，在命令提示符下输入如下命令：

```
dsquery group DC=coolpen,DC=net
```

按回车键，显示当前域中的所有组，如图 2-79 所示。

dsquery group 的语法格式为：

```
dsquery group [{StartNode| forestroot | domainroot}] [-o {dn | rdn | samid}] [-scope {subtree | onelevel | base}] [-name Filter] [-desc Filter] [-samid Filter] [{-s Server| -d Domain}] [-u UserName] [-p {Password| *}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

dsquery group 命令中各参数的使用方法和 dsquery computer 命令相同，可参阅前面所述内容，此

处不再重复。

4. dsquery ou——显示组织单位

dsquery ou 命令用来在域中查找并显示组织单位。

例如查找当前域中所有的组织单位，在命令提示符下输入如下命令：

```
dsquery ou
```

按回车键，显示当前域中所有的组织单位，如图 2-80 所示。

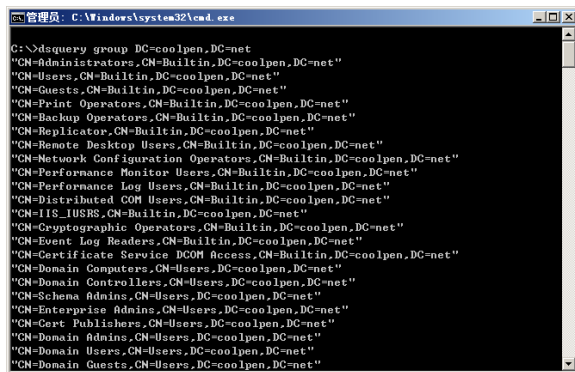


图 2-79 域中的所有组

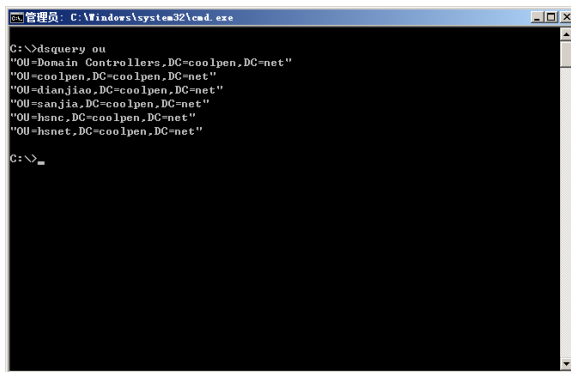


图 2-80 当前域中的所有组织单位

例如在当前域中查找所有名称以“hs”开头的组织单位，在命令提示符下输入如下命令：

```
dsquery ou domainroot -name hs*
```

按回车键，显示当前域中所有名称以“hs”开头的组织单位，如图 2-81 所示。

dsquery ou 的语法格式为：

```
dsquery ou [{StartNode| forestroot | domainroot}] [-o {dn | rdn}][--scope {subtree | onelevel | base}][--name Name] [--desc Description] [{-s Server| -d Domain}] [-u UserName] [-p {Password| *}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

参数说明如下。

(1) -name Name: 搜索组织单位，其中 Name 表示组织单位名称。

(2) -desc Description: 根据组织单位的描述搜索，其中 Description 表示组织单位名称。

dsquery ou 命令中其他参数的使用方法和 dsquery computer 命令相同，可参阅前面所述内容，此处不再重复。

5. dsquery partition——查找分区对象

dsquery partition 命令用来在域中查找分区对象，如果该命令中预定义的搜索条件不充分，可以使用 dsquery *命令查询。

例如，要列出当前目录林中所有的分区信息，可在命令提示符下输入如下命令：

```
dsquery partition
```

按回车键，显示当前目录林中所有的目录分区，如图 2-82 所示。

dsquery partition 命令的语法格式为：

```
dsquery partition [-o {dn | rdn}] [-part Filter] [{-s Server| -d Domain}] [-u UserName] [-p {Password|*}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

参数说明如下。

(1) -part Filter: 要查找的分区名称。

(2) {-s Server| -d Domain}: 连接到指定远程服务器或域，默认连接当前登录域中的域控制器。

dsquery partition 命令中其他参数请参阅前面所述内容，此处不再重复。

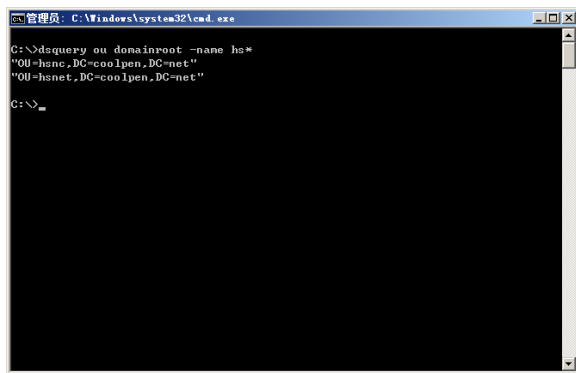


图 2-81 当前域中所有名称以“hs”开头的组织单位

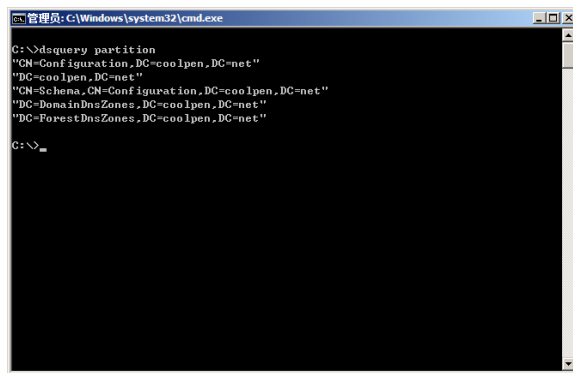


图 2-82 当前目录林中所有的分区信息

6. dsquery quota——查找配额规范

dsquery quota 命令用来在域中查找配额，配额规范确定安全主体在给定目录分区中可以拥有的目录对象的最大数量。

例如，要列出已将配额规范分配至的当前域中的所有账户，在命令提示符下输入如下命令：

```
dsquery quota domainroot
```

按回车键，由于没有配置目录配额，因此没有找到符合条件的已经分配的当前域中的所有账户，如图 2-83 所示。

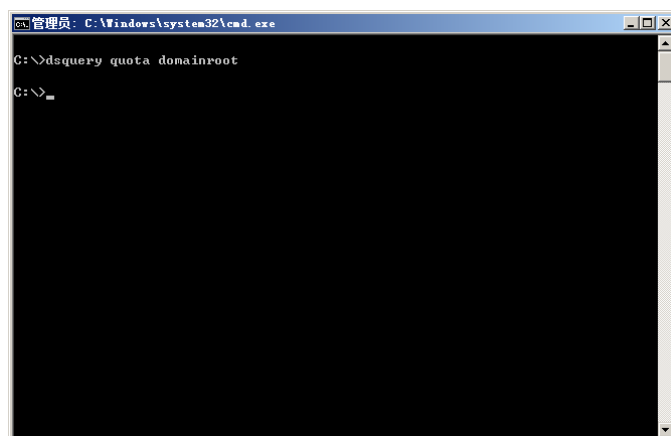


图 2-83 未找到账户

dsquery quota 命令的语法格式为：

```
dsquery quota {domainroot |ObjectDN} [-o {dn | rdn}] [-acct Name] [-qlimit Filter]
[-desc Description] [{-s Server| -d Domain}] [-u UserName] [-p {Password|*}] [-q] [-r]
[-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

参数说明如下。

(1) {domainroot |ObjectDN}：必需项，指定搜索的开始位置。ObjectDN 用来指定可分辨名称，domainroot 用来指定当前域的根目录。

(2) -acct Name：指定要查找分配给安全主体（用户、组、计算机或 InetOrgPerson）的配额规范，该安全主体由 Name 表示。-acct 选项由安全主体的可分辨名称或安全主体的 Domain\SAMAccountName 提供。

(3) -qlimit Filter：指定要查找其限制匹配 Filter 的配额规范。

(4) -desc Description：搜索描述属性与 Description 相匹配的配额对象。

dsquery quota 命令中其他参数的使用方法请参阅前面所述内容，此处不再重复。

7. dsquery server——查找域控制器

dsquery server 用来按照指定的搜索条件查找域控制器。如果该命令中预定义的搜索条件不充分，可以使用该查询命令的更常规的形式 dsquery *。

例如查找当前域中所有的域控制器，在命令提示符下输入如下命令：

```
dsquery server
```

按回车键，列出当前域中所有的域控制器，如图 2-84 所示。

例如查找林中的所有域控制器并显示其相对可分辨名称，在命令提示符下输入如下命令：

```
dsquery server -o rdn -forest
```

按回车键，显示林中的域控制器，如图 2-85 所示。

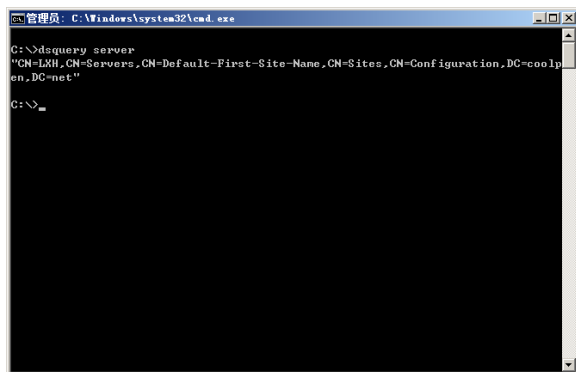


图 2-84 当前域中所有的域控制器

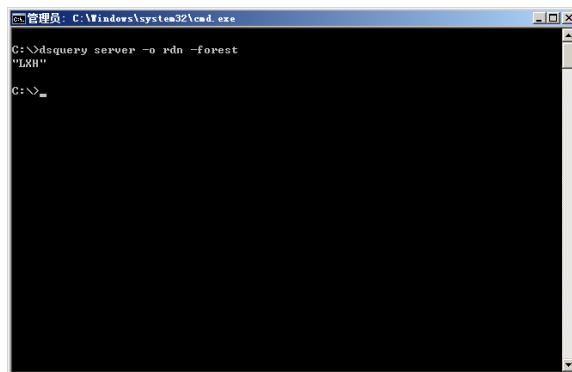


图 2-85 林中的域控制器

例如查找林中具有架构操作主机角色的域控制器，在命令提示符下输入如下命令：

```
dsquery server -forest -hasfsmo schema
```

按回车键，命令成功执行，列出林中具有架构操作主机角色的域控制器，如图 2-86 所示。

例如查找指定域 coolpen.net 中的所有域控制器，在命令提示符下输入如下命令：

```
dsquery server -domain coolpen.net
```

按回车键，列出域 coolpen.net 中的域控制器，如图 2-87 所示。

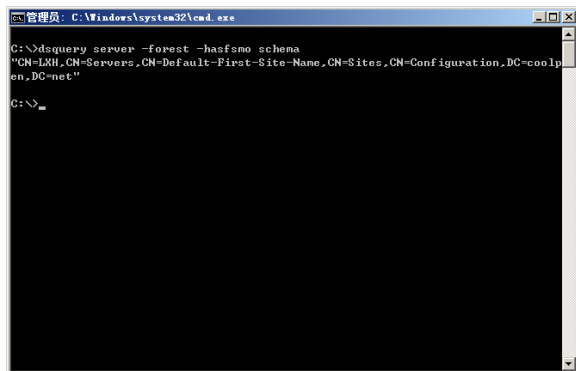


图 2-86 林中具有架构操作主机角色的域控制器

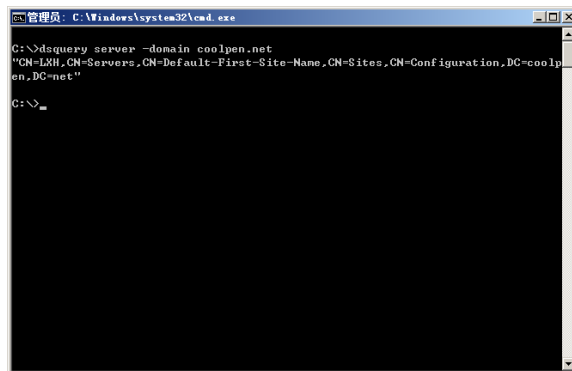


图 2-87 域 coolpen.net 中的控制器

dsquery server 的语法格式为：

```
dsquery server [-o {dn | rdn}] [-forest] [-domain DomainName] [-site SiteName] [-name Name] [-desc Description] [-hasfsmo {schema | name | infr | pdc | rid}] [-isgc] [{-s Server | -d Domain}] [-u UserName] [-p {Password|*}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

参数说明如下。

- (1) **-forest**: 搜索属于当前林的所有域控制器（服务器对象）。
- (2) **-domain DomainName**: 搜索指定域（由 DomainName 指定）中的所有域控制器。如果要查找当前域中的所有域控制器，可不加此参数。
- (3) **-site SiteName**: 搜索指定站点的所有域控制器。
- (4) **-name Name**: 根据名称搜索服务器对象。
- (5) **[-hasfsmo {schema | name | infr | pdc | rid}]**: 搜索操作主机角色的域控制器。schema 请求林的架构主机，name 请求林的域命名主机，infr 请求林的结构主机，pdc 请求由-domain 参数（或当前域）指定的域的主域控制器（PDC）角色所有者，rid 请求由-domain 参数（或当前域）指定的域的相对 ID 主机（RID 主机）。对于 infr、pdc 和 rid 操作主机角色，如果未使用-domain 参数指定域，则使用当前域。
- (6) **-isgc**: 在全局编录服务器的-forest、-domain 或-site 参数指定的范围中搜索所有域控制器（服务器对象）。如果未指定参数，则从当前域中查找。

dsquery quota 命令中其他参数的使用方法请参阅前面所述内容，此处不再重复。

8. dsquery site——查找站点

dsquery site 命令用来在域中查找站点。

例如在域 coolpen.net 中查找名称以“Default”开头的所有站点，在命令提示符下输入如下命令：

```
dsquery site -name Default*
```

按回车键，列出域 coolpen.net 中以“Default”开头站点，如图 2-88 所示。

例如列出域 coolpen.net 中定义的所有站点的相对可分辨名称，在命令提示符下输入如下命令：

```
dsquery site -o rdn
```

按回车键，列出域中所有站点的相对可分辨名称，如图 2-89 所示。

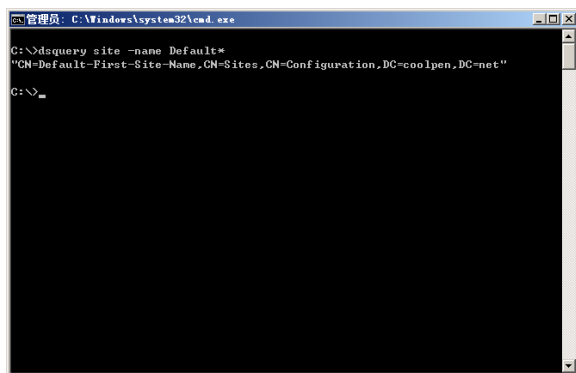


图 2-88 域 coolpen.net 中以“Default”开头站点

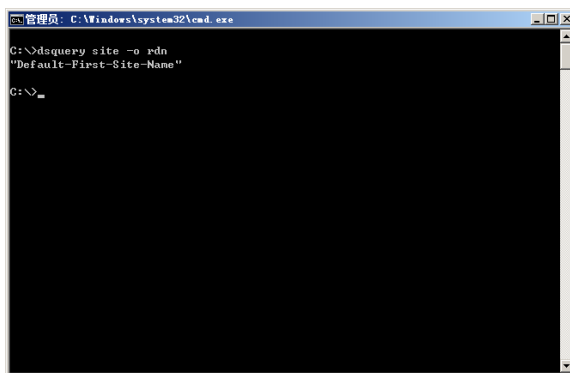


图 2-89 域中所有站点的相对可分辨名称

dsquery site 命令的格式为

```
dsquery site [-o {dn | rdn}] [-name Name] [-desc Description] [{-s Server | -d Domain}] [-u UserName] [-p {Password|*}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco | -uci}]
```

其中各参数的使用方法请参阅前面所述内容，此处不再重复。

9. dsquery * ——查找目录中的任何对象

dsquery * 命令用来在目录中按照使用 LDAP 查询条件查找目录中的任何对象。

例如查找域中的所有对象，在命令提示符下输入如下命令：

```
dsquery *
```

按回车键，显示当前域中的所有对象，如图 2-90 所示。

例如查看域 coolpen.net 的组织单位 book 中对象的所有属性，在命令提示符下输入如下命令：


```
dsquery * OU=book,DC=coolpen,DC=net -scope base -attr *
```

按回车键，显示组织单位 book 的所有属性。如名称及创建时间等信息，如图 2-91 所示。

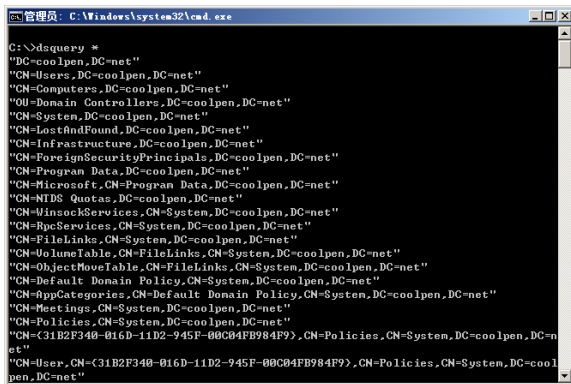


图 2-90 域中的所有对象

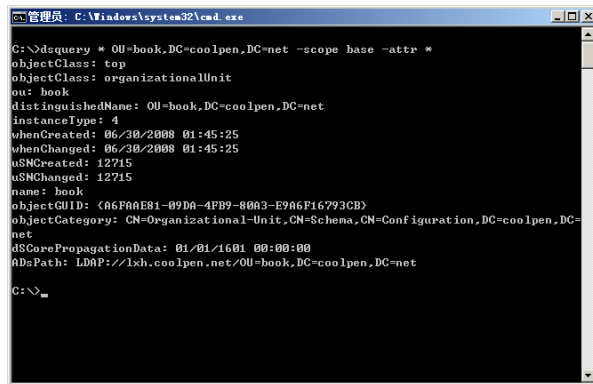


图 2-91 组织单位 book 的所有属性

dsquery *命令的语法格式为：

```
dsquery * [{ObjectDN| forestroot | domainroot}] [-scope {subtree | onelevel | base}]
[-filter LDAPFilter] [-attr {AttributeList|*}] [-attrsonly] [-l] [{-s Server| -d Domain}]
[-u UserName] [-p {Password|*}] [-q] [-r] [-gc] [-limit NumberOfObjects] [{-uc | -uco |
-uci}]
```

参数说明如下。

(1) {ObjectDN| forestroot | domainroot}：指定开始搜索的节点。可以指定森林根目录（forestroot）、域根目录（domainroot）或节点的可分辨名称。如果指定了 forestroot，则使用全局编录完成搜索。默认为 domainroot。

(2) -filter LDAPFilter：指定显式搜索筛选器 LDAPFilter（以 LDAP 搜索筛选格式指定用于此搜索）。例如，(&(objectCategory=Person)(sn=smith*))。默认的 LDAPFilter 是 (objectClass=*)。

(3) -attr {AttributeList|*}：指定 AttributeList 中包含的以分号分隔的 LDAP 显示名是结果集中应该显示的每个条目的唯一属性。如果参数为*，则显示所有属性。如果选择此选项，则无论是否指定-L 参数，默认的输出格式为列表格式。默认的 AttributeList 是可分辨名称。

(4) -attrsonly：指定只显示条目的属性类型，而不显示属性值。默认情况下，属性类型和属性值均显示。

(5) -l：以列表格式显示，默认以表格形式。

dsquery * 命令中其他参数的使用方法请参阅前面所述内容，此处不再重复。

10. dsquery user——查找用户

dsquery user 用来在目录中查找与指定的搜索条件相匹配的用户。

例如查找组织单位 coolpen 中名称以“hs”开头且被禁止登录的用户，在命令提示符下输入如下命令：

```
dsquery user OU=book,DC=coolpen,DC=net -o upn -name hs* -disabled
```

按回车键，显示所有名称以“hs”开头且被禁止登录的用户账户，如图 2-92 所示。

例如显示组织单位 book 中所有用户的主体名称，在命令提示符下输入如下命令：

```
dsquery user OU=book,DC=coolpen,DC=net -o upn
```

按回车键，显示组织单位中的所有用户，如图 2-93 所示。

Dsquery User 命令的格式为：

```
dsquery user [{StartNode| forestroot | domainroot}] [-o {dn | rdn | upn | samid}] [-scope
{subtree | onelevel | base}] [-name Name] [-desc Description] [-upn UPN] [-samid SAMName]
```

```
[ -inactive NumberOfWeeks] [ -stalepwd NumberOfDays] [ -disabled] [{ -s Server | -d Domain}]  
[ -u UserName] [ -p {Password | *} ] [ -q] [ -r] [ -gc] [ -limit NumberOfObjects] [{ -uc | -uco  
| -uci}]
```

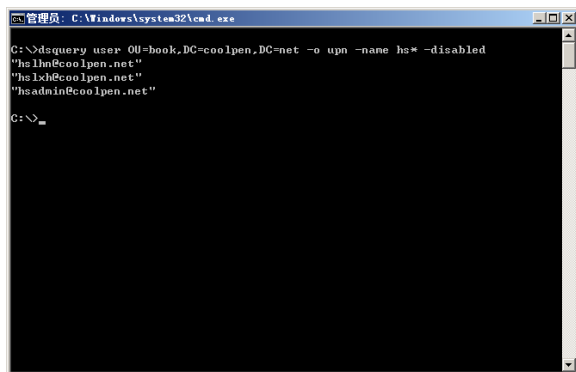


图 2-92 所有名称以“hs”开头且被禁止登录的用户账户

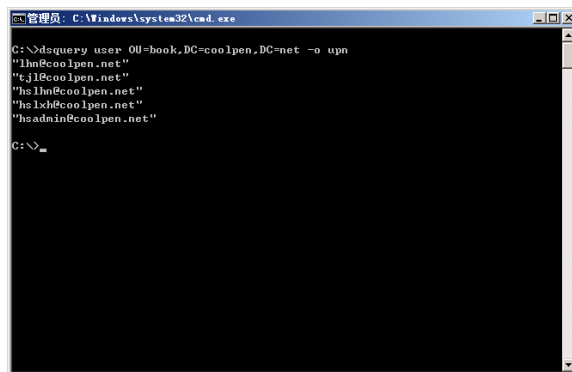


图 2-93 组织单位中的所有用户

参数说明如下。

- (1) **-name Name**: 根据指定的名称搜索用户。
- (2) **-desc Description**: 根据描述属性搜索用户。
- (3) **-upn UPN**: 根据 UPN 属性搜索用户。
- (4) **-samid SAMName**: 根据 SAM 账户名搜索用户。
- (5) **-inactive NumberOfWeeks**: 搜索至少在指定的周数内处于非活动状态的用户。
- (6) **-stalepwd NumberOfDays**: 搜索至少在指定天数内未更改密码的用户。
- (7) **-disabled**: 搜索已禁用的用户。

dsquery user 命令中其他参数的使用方法请参阅前面所述内容，此处不再重复。

第3章 配置与管理活动目录服务

活动目录（Active Directory）是 Windows Server 系统中重要的目录服务，用于管理网络中的用户和资源，如计算机、打印机或应用程序等。Windows Server 2008 中的 Active Directory 域服务包含了早期 Windows 版本中活动目录所没有的新特性，如 Active Directory RMS 服务、Active Directory 联合身份验证服务、Active Directory 轻型目录服务器和 Active Directory 证书服务等实用功能组件。从而使得管理员能够更简单且更安全地部署各种服务，并更有效地进行管理。

3.1 活动目录概述

活动目录是 Windows Server 系统中重要的目录服务，存储了网络上各种资源信息。只要拥有相应的权限，管理员或用户在网络中的任何一台计算机上都可以登录到域，并查询和使用这些信息。

3.1.1 活动目录的重要意义

活动目录中存储了所有用户的信息，并负责目录数据库的保存、新建、删除、修改与查询等，使其用户很容易地在目录内寻找所需要的数据。

活动目录具有以下意义。

（1）简化管理

活动目录和域密切相关，域指网络服务器和其他计算机的一种逻辑分组。凡是在共享域逻辑范围内的用户都使用公共的安全机制和用户账户信息，每个使用者在域中只拥有一个账户，每次登录的是整个域。

活动目录用于将域中的资源分层次地组织在一起，每个域都包含一个或多个域控制器。域控制器即运行 Windows Server 2008 的计算机，其中存储域目录的一份完整的副本。为了简化管理，域中的所有域控制器都是对等的，可以在任意一台域控制器上修改，更新的内容将被复制到该域中的所有其他域控制器。活动目录为管理网络上的所有资源提供一个单一入口，因而进一步简化了管理，管理员可以登录任意一台计算机并管理网络中任何计算机上的对象。

（2）安全性

安全性通过登录身份验证及目录对象的访问控制集成在活动目录之中，通过单点网络登录管理员可以管理分散在网络各处的目录数据和组织单位，经过授权的网络用户可以访问网络任意位置的资源。基于策略的管理则简化了网络的管理，即便是那些最复杂的网络也是如此。

活动目录通过对象访问控制列表及用户凭据保护其存储的用户账户和组信息，因为活动目录不但可以保存用户凭据，而且可以保存访问控制信息。所以登录到网络上的用户既能够获得身份验证，也可以获得访问系统资源所需的权限。例如，在用户登录到网络时，安全系统首先会利用存储在活动目录中的信息验证用户的身份。然后在用户试图访问网络服务时，系统会检查在服务的自由访问控制列表（DCAL）中所定义的属性。

由于活动目录允许管理员创建组账户，所以管理员可以更加有效地管理系统的安全性，通过控制组权限即可控制组成员的访问操作。

（3）改进的性能与可靠性

Windows Server 2008 能够更加有效地管理活动目录的复制与同步，无论是在域内还是在域间，管

理员都可以更好地控制要在域控制器间进行同步的信息类型。此外活动目录还提供了许多技术，可以智能地选择只复制那些发生了更改的信息，而不是机械地复制整个目录的数据库。

3.1.2 活动目录对象

活动目录对象是指域控制器中包含相同属性的实体组成的集合，例如计算机、用户及打印机等。每个对象都有相应的属性，用来描述目录对象可以标识的数据，例如用户的属性包括用户姓名和电子邮件地址等。

1. 默认容器对象

在安装活动目录过程中已经自动创建了一些默认的容器（Container）对象，这些容器对象中都包括一组属性相似的活动目录对象，也可以包含其他容器。这些默认容器对象通常用来存储常用的网络资源，用户也可以根据自己的需要创建新的容器来存储特定类型的资源。

(1) Builtin 容器

Builtin 是 Active Directory 默认创建的第 1 个容器，主要用于保存域中本地安全组的子对象，如图 3-1 所示。默认情况下，不同默认用户组中的成员权限也不同，并且在 Active Directory 默认提供的容器中，这是唯一一个用户无法将默认对象删除或移动的容器。

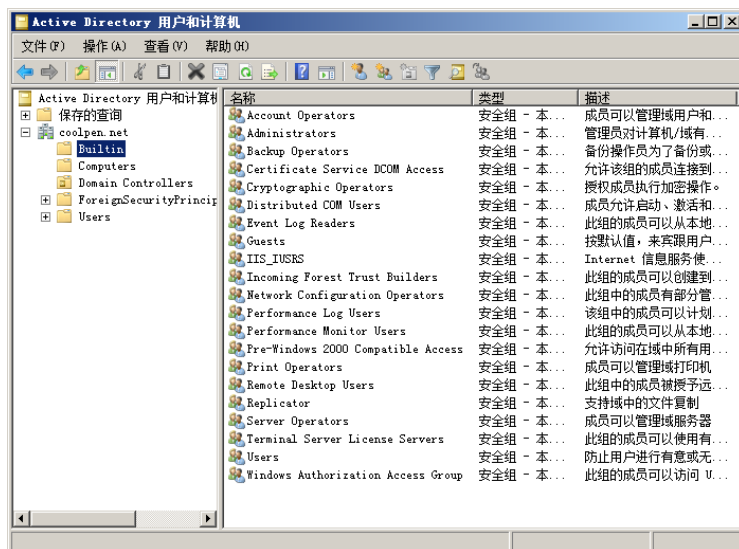


图 3-1 Builtin 容器

Builtin 容器中包括以下默认用户组。

➤ Account Operators

该组的成员可以创建、修改和删除位于“Users”或“Computers”容器中的用户、组和计算机的账户，以及该域中的组织单位，但“Domain Controllers”组织单位除外。该组的成员无权修改 Administrators 或 Domain Admins 组，也无权修改这些组的成员账户。这些成员可本地登录到该域的域控制器中，并可将其关闭。

➤ Administrators

该组的成员具有对域中所有域控制器的完全控制。默认情况下，Domain Admins 和 Enterprise Admins 组是 Administrators 组的成员。Administrator 账户也是默认成员。

➤ Backup Operators

该组的成员可备份和还原该域中域控制器上的所有文件，而不用考虑其各自拥有的这些文件的权限。Backup Operators 还可以登录到域控制器并将其关闭，它没有默认的成员。

➤ Guests

默认情况下，Domain Guests 组是该组的成员，Guest 账户（默认情况下禁用此账户）也是其默认成员。

➤ Incoming Forest Trust Builders（仅出现在林根域中）

该组的成员可创建对林根域的单向传入林信任，例如，驻留在 A 林中的该组成员能够创建来自 B 林的单向传入林信任。该单向传入林信任允许 A 林中的用户访问位于 B 林中的资源，该组的成员在林根域上会得到“创建传入林信任”权限。该组没有默认的成员。

➤ Network Configuration Operators

该组的成员可更改 TCP/IP 设置并续订和发布该域中域控制器上的 TCP/IP 地址，该组没有默认的成员。

➤ Performance Monitor Users

该组的成员可在本地或从远程客户端监视该域中域控制器上的性能计数器，不必成为 Administrators 或 Performance Log Users 组的成员。

➤ Performance Log Users

该组的成员可在本地或从远程客户端管理该域中域控制器上的性能计数器、日志和警报，不必成为 Administrators 组的成员。

➤ Pre-Windows 2000 Compatible Access

该组的成员具有对该域中所有用户和组的读取访问权限，该组向后兼容运行 Windows NT 4.0 及更低版本的计算机。默认情况下，特殊的 Everyone 标识是该组的成员。仅当用户在运行 Windows NT 4.0 或更低版本时才将其添加到该组中。

➤ Print Operators

该组的成员可管理、创建、共享和删除连接到该域中域控制器上的打印机，它们可以管理该域中的 Active Directory 打印机对象，也可本地登录到该域的域控制器中并可将其关闭。该组没有默认的成员。

➤ Remote Desktop Users

该组的成员可远程登录到该域的域控制器，该组没有默认的成员。

➤ Replicator

该组支持目录复制功能，并由该域的域控制器上的“文件复制”服务使用。该组没有默认的成员，不在其中添加用户。

➤ Server Operators

在域控制器上，该组的成员可进行交互式登录、创建和删除共享资源、启动和停止某些服务、备份和还原文件、格式化硬盘，以及关闭计算机等。该组没有默认的成员。

➤ Users（用户）

该组的成员可执行大部分常见任务，如运行应用程序、使用本地和网络打印机，以及锁定服务器等。默认情况下，Domain Users 组、Authenticated Users 或 Interactive 都是该组的成员，因此域中创建的任意用户账户均为该组成员。

■ 提示



由于该容器中的所有用户组都是系统默认创建的，因此对于控制器有非常重要的作用，操作时应加倍谨慎。

（2）Computers 容器

Computers 容器是 Active Directory 默认提供的第 2 个容器，用于存放域中所有成员计算机的账户，如图 3-2 所示。如果使用拥有足够权限的用户账户登录到域控制器，就可以直接管理这些成员计算机。

(3) Domain Controllers 容器

Domain Controllers 是一个特殊的容器，确切地说是一个组织单元 (Organizational Unit, OU)。OU 是活动目录中比较特殊的容器，其中除了可以包含其他对象和组织单位之外，还有“组准则”的功能。Domain Controllers 容器也是 Active Directory 默认生成的容器之一，主要用于存放当前域控制器下创建的所有子域和辅助域，如图 3-3 所示。

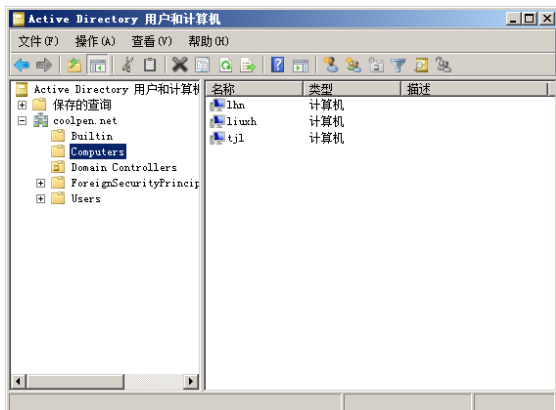


图 3-2 Computers 容器

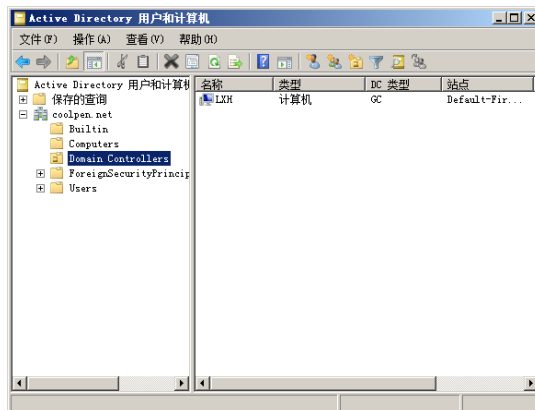


图 3-3 Domain Controllers 容器

(4) Users 容器

Users 容器主要用于存放安装 Active Directory 时系统自动创建的用户组和登录到当前域控制器的所有用户账户，如图 3-4 所示。

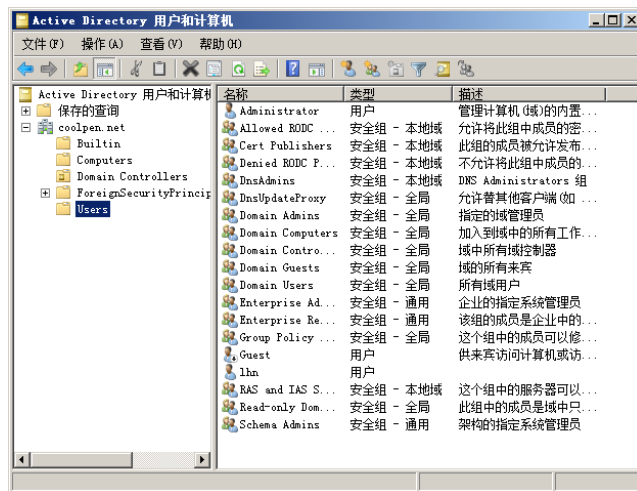


图 3-4 Users 容器

Users 容器中默认创建的用户和用户组如下。

- Cert Publishers: 成员获准为用户和计算机发行证书。
- DnsAdmins (随 DNS 安装): 成员具有对 DNS Server 服务的管理访问权。
- DnsUpdateProxy (随 DNS 安装): 成员是可代表其他客户端 (如 DHCP 服务器) 执行动态更新的 DNS 客户端。
- Domain Admins: 成员具有对该域的完全控制权。
- Domain Computers: 包含加入到此域的所有工作站和服务器。
- Domain Controllers: 包含此域中的所有域控制器。
- Domain Guests: 包含所有域来宾。
- Domain Users: 包含所有域用户。

- Enterprise Admins（仅出现在林根域中）：成员具有对林中所有域的完全控制作用。
- Group Policy Creator Owners：成员可修改此域中的组策略。
- IIS_WPG（随 IIS 安装）：IIS_WPG 组是 Internet 信息服务（IIS 6.0）辅助进程组。
- RAS 和 IAS Servers：该组中的服务器获准访问用户的远程访问属性。
- Schema Admins（仅出现在林根域中）：成员可修改 Active Directory 架构。

2. 活动目录对象

在活动目录数据库中允许用户创建各种对象，用于实现不同的功能。可以创建的活动目录对象如下。

- （1）计算机：代表网络上的计算机资源。
- （2）联系人：一个没有任何安全权限的账户，不能以联系人的身份登录到域，通常用于 E-mail 联系。
- （3）组：容器对象，可以容纳用户和计算机等对象。
- （4）组织单位：容器对象，用来把其他活动目录容器和叶子对象逻辑的组织在一起，就像是 Windows 资源管理器中的文件夹。
- （5）打印机：用户对象，是活动目录中的安全主体。以客户端都必须凭据有效的用户名和密码登录到域控制器，并且可以为不同的用户分配不同的访问权限。
- （6）用户：用户登录域的账户。
- （7）共享文件夹：代表网络中的共享文件夹。

3.1.3 活动目录组件

在默认的安装过程中，无论计算机是否是域的成员，都将安装 Active Directory 集成子组件。

如果在 Windows Server 2000/2003/2008 域的成员计算机上安装消息队列，则可通过安装 Active Directory 集成子组件来指定计算机是否在域模式下运行。如果未安装该子组件，计算机将在工作组模式下运行。在消息队列上下文中可将工作组模式定义为任何不允许访问目录服务的操作模式，即使使用的计算机属于某个域，工作组操作模式要求直接连接以便发送消息。

如果在属于域的计算机上安装消息队列，而且选择 Active Directory 集成子组件（与默认配置相同），则安装程序将尝试与本地站点或附近站点的域控制器联系。如果联系成功，则计算机将在域模式下运行。同时启用对 Active Directory 的访问，而且将在 Active Directory 中创建 MSMQ 对象。注意，只能自动查找 Windows Server 2003 或 Windows 2000 Server 域控制器。如果无法定位其中的某个域控制器，则系统将提示输入本地站点中的 MSMQ 1.0 PEC 或 PSC（在 Windows NT 4.0 Enterprise 中）的名称。如果没有提供这样的名称，而且继续操作，则将以工作组模式安装消息队列。在这种情况下，当计算机属于某个域，而且安装了 Active Directory 集成子组件，但暂时无法访问域控制器时，计算机将以工作组模式工作。不过下次重新启动这样的计算机，或者停止并重新启动消息队列服务时，消息队列将自动尝试与本地域中的域控制器联系。如果域控制器可用，而且联系成功，则计算机将在域模式下运行。

如果计算机不属于域，则 Active Directory 集成子组件的默认安装允许此计算机可能在以后加入某个域。

3.1.4 活动目录结构

活动目录结构主要是指网络中所有用户、计算机，以及其他网络资源的层次关系，就像是一个大型仓库中分出若干个小的储藏间，每一个小储藏间分别用来存放哪些物品一样。通常活动目录的结构可以分为逻辑结构和物理结构，分别包含不同的对象。

1. 逻辑结构

活动目录的逻辑结构非常灵活，其中的逻辑单元包括域、OU、域树和域林。

(1) 域

域既是活动目录中的逻辑组织单元，也是网络的安全边界。域管理员只能管理域的内部，除非其他域赋予了管理权限；否则不能访问或管理其他域。每个域都有自己的安全策略，以及与其他域的安全信任关系。

在活动目录的复制过程中，域也是一个重要的单元。由于活动目录采用了多主机的复制模式，所以在域中每个域控制器既可以接收来自域中其他域控制器的变化信息，也可以把变化的信息复制到其他域控制器上。

(2) OU

OU 是一个容器对象，可以包含各种对象，如用户账户、用户组、计算机、打印机，甚至其他 OU，所以可以利用 OU 把域中的对象形成一个完全逻辑上的层次结构。对于企业来讲，可以按部门把所有的用户和设备组成一个 OU 层次结构，也可以按地理位置、功能和权限分成多个 OU 层次结构。图 3-5 所示为域控制器下包括的 3 个 OU。

由于 OU 层次结构局限于域的内部，所以一个域中的 OU 层次结构与另一个域中的 OU 层次结构没有任何关系。就像是 Windows 资源管理器中位于不同目录下的文件，可以重名或重复。

(3) 域树

域树是活动目录中共享连续名字空间的层次结构，从根域开始每加入一个域，新域就成为树中的一个子域。例如，he.coolpen.net 为 coolpen.net 的子域及 hs.he.coolpen.net 的父域。coolpen.net 域为 he.coolpen.net 的父域，也是该域树的根域，如图 3-6 所示。

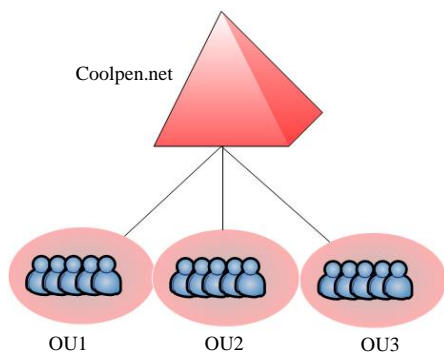


图 3-5 域中控制器下的 3 个 OU

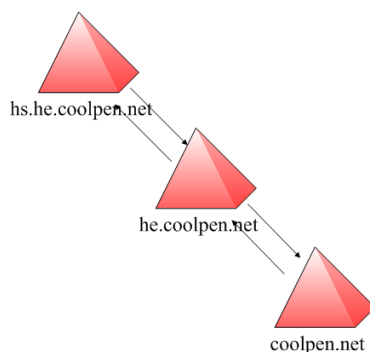


图 3-6 域树

域树中的多个域通过双向可传递信任关系连接在一起，因此在域树或树林中新创建的域可以与域树或树林中其他域建立信任关系，允许在所有域上对用户进行身份验证。不过由于域是安全界限，可以用户必须在每个域的基础上指定权利和权限。

(4) 域林

域林是活动目录中不共享连续名字空间的域树组成的结构，但是域林中的每个域树相互信任，共享同一套配置、表结构，以及全局目录。默认情况下，域林中第 1 个域树的名字也被作为域林的名字。图 3-7 所示是有 3 个域树构成的一个简单域林。

2. 物理结构

活动目录的物理结构与逻辑结构有很大不同，是彼此独立的两个概念。逻辑结构侧重于网络资源的管理；物理结构则侧重于活动目录信息的复制和用户登录网络时的性能优化，物理结构的两个重要概念是站点和域控制器。

(1) 站点

站点由一个或多个 IP 子网组成，这些子网通过高速网络设备连接在一起。站点往往由企业的物理位置分布情况决定，可以依据站点结构配置活动目录的访问和复制拓扑关系。这样能使得网络更有效地连接，并且可使复制策略更合理，用户登录更快速。活动目录中的站点与域是两个完全独立的概念，

一个站点中可以有多个域，多个站点也可以位于同一域中。

活动目录站点和服务可以通过使用站点提高大多数配置目录服务的效率，通过使用活动目录站点和服务来发布站点并提供有关网络物理结构的信息，从而确定如何复制目录信息和处理服务的请求。计算机站点是根据其在子网或一组已连接子网中的位置指定的，子网用来为网络分组，类似于生活中使用邮政编码划分地址。划分子网可方便发送有关网络与目录连接物理信息，而且同一子网中计算机的连接情况通常优于不同网络。

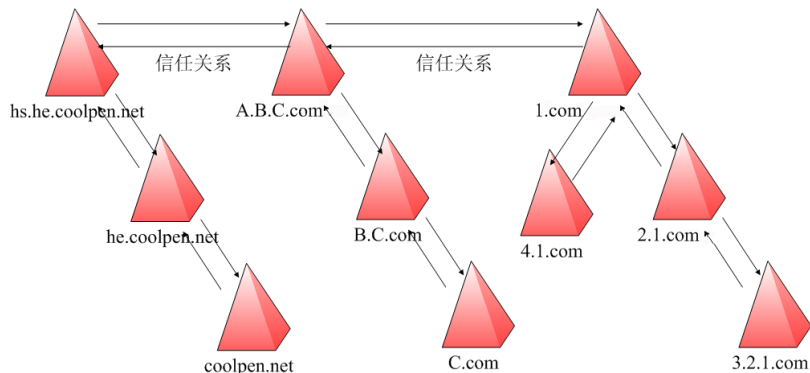


图 3-7 3 个域构成的一个简单域林

使用站点具有如下意义。

➤ 提高了验证过程的效率

当客户使用域账户登录时，登录机制首先搜索与客户处于同一站点内的域控制器，以使网络传输本地化。从而加快身份验证的速度，提高验证过程的效率。

➤ 平衡了复制频率

活动目录信息可在站点内部或站点之间复制信息，但由于网络的原因，活动目录在站点内部复制信息的频率高于站点间的复制频率，这样做可以平衡对最新目录信息需求和可用网络带宽带来的限制。可通过站点链接来定制活动目录如何复制信息以指定站点的连接方法，活动目录使用有关站点如何连接的信息生成连接对象以提供有效的复制和容错。

➤ 可提供有关站点链接信息

活动目录可使用站点链接信息费用、链接使用次数、链接何时可用，以及链接使用频度等信息确定应使用哪个站点来复制信息，以及何时使用该站点，定制复制计划使复制在特定时间（诸如网络传输空闲时）进行会使复制更为有效。通常所有域控制器都可用于站点间信息的交换，但也可以通过指定桥头堡服务器优先发送和接收站间复制信息的方法进一步控制复制行为。当拥有希望用于站间复制的特定服务器时，宁愿建立一个桥头堡服务器，而不使用其他可用服务器。或在配置使用代理服务器时建立一个桥头堡服务器，用于通过防火墙发送和接收信息。

(2) 域控制器

域控制器指运行 Windows Server 2000/2003/2008 的服务器，其中保存活动目录信息的副本。它管理目录信息的变化，并把这些变化复制到同一个域中的其他域控制器上，使各域控制器上的目录信息保持同步。域控制器也负责用户的登录过程及其他与域有关的操作，如身份鉴定及目录信息查找等。一个域可以有多个域控制器，规模较小的域可以只需要两个域控制器，一个实际使用，另一个用于容错性检查；规模较大的域可以使用多个域控制器。

尽管活动目录支持多主机复制方案，然而由于复制引起的通信流量，以及网络潜在的冲突，变化的传播并不一定能够顺利进行。因此需要在域控制器中指定全局目录服务器及操作主机。全局目录是一个信息仓库，包含活动目录中所有对象的一部分属性，并且往往是在查询过程中访问最为频繁的属性。利用这些信息，可以定位到任何一个对象的实际位置。而全局目录服务器是一个域控制器，其中

保存全局目录的一份副本，并执行全局目录的查询操作。该服务器可以提高检索活动目录中大范围内对象的性能，如果没有全局目录服务器，那么查询操作必须要调动域林中每一个域的查询过程；如果域中只有一个域控制器，那么它就是全局目录服务器；如果有多个域控制器，那么管理员必须把一个域控制器配置为全局目录控制器。

3.1.5 复制活动目录

复制指将更新的数据从源计算机上的数据存储或文件系统复制到一台或多台目标计算机上匹配的数据存储或文件系统，从而同步这些数据的过程，因此有时也称为“服务器同步”。在 Active Directory 中通常是指域控制器间的复制同步架构、配置和域目录分区。通过复制，Active Directory 目录服务在多个域控制器上保留目录数据的副本，从而确保所有用户的目录可用性和性能。Active Directory 使用一种多主机复制模型，允许在任何域控制器上（而不只是委派的主域控制器上）更改目录。它依靠站点概念来保持复制的效率，并依靠信息一致性检查器（KCC）来自动确定网络的最佳复制拓扑。

1. 组织复制数据

数据存储在每个域控制器中，目录存储在逻辑上分成特定的目录分区中。每个分区存储一种不同类型的目录数据，比如域数据、林架构数据、林配置数据或应用程序数据。林中的所有域控制器都拥有该林的架构和配置分区的副本，而特定域中的所有域控制器都拥有该域的域分区的副本。应用程序目录分区拥有应用程序特定的目录数据，并可由属于不同域的域控制器存储。对每个目录分区的更改将被复制到拥有该分区副本的所有其他域控制器。

复制还确保了整个林的全局编录的可用性，全局编录是可搜索的目录存储，其中包含所有域中每个对象的相关数据。全局编录由已经为其启用了该全局编录的域控制器存储。

2. 利用站点提高复制效率

Active Directory 依靠站点使复制更加有效，站点决定了目录数据的复制方式。Active Directory 在一个站点内比在站点之间更频繁地复制目录信息，这样连接最好的域控制器中最可能需要特定目录信息的域控制器首先接收复制的更新内容。其他站点中的域控制器也接收更改，但不频繁，以降低网络带宽的消耗。

3. 确定复制拓扑

信息一致性检查器（KCC）是运行在每个域控制器中的一个进程，它根据用户在“Active Directory 站点和服务”中提供的网络信息自动为网络确定最有效的复制拓扑。KCC 定期计算复制拓扑以便针对所发生的任何网络更改而做出调整，每个站点中一个域控制器的 KCC（站点间拓扑生成程序）决定了站点间的复制拓扑。

3.1.6 命名规范

Active Directory 中的每个对象都可通过多种不同的名称引用，Active Directory 根据对象创建或修改时提供的信息为每个对象创建相对可分辨名称和规范名称。每个对象也可通过其可分辨名称引用，该名称是从该对象及其所有父容器对象的相对可分辨名称中获得的。

LDAP 相对可分辨名称唯一标识其父容器中的对象，例如，名为“hscoolpen”的计算机的 LDAP 相对可分辨名称是“CN=hscoolpen”。相对可分辨名称必须唯一，用户不能在组织单位中有相同的名称。

LDAP 可分辨名称是全局唯一的，例如，在 coolpen.net 域且 book 组织单位中名为“hscoolpen”的计算机的可分辨名称是“CN=hscoolpen,OU=book,DC=coolpen,DC=net”。

规范名称是按照可分辨名称的同一方法构造的，但用不同的方法表示，在上例中计算机的规范名称是“coolpen.net/book/hscoolpen”。

安全主体对象是指派了安全 ID（SID）、可用于登录到网络并可被指派域资源访问权限的 Active

Directory 对象，管理员只需要为域中唯一的安全主体对象（用户账户、计算机账户和组）提供名称。

在目录添加新用户账户时，用户登录网络必须使用的名称、包含用户账户和其他说明性数据（如名字、姓氏和电话号码等）的域的名称等信息都记录在目录中。

安全主体对象的名称可以包含除了 RFC 2253 中定义的特殊 LDAP 字符以外的所有 Unicode 字符，这个特殊字符列表包含前导空格、尾随空格，以及字符#、,、+、"、\、<、>和；等。

安全主体名称必须符合如表 3-1 所示的原则。

表 3-1 Active Directory 安全主体命名原则

账户名类型	最大尺寸	特殊限制
用户账户	运行 Windows Server 2000/2003/2008 的计算机可使用用户账户的用户主体名称 (UPN)，运行 Windows NT 4.0 及其以前版本的计算机仅限于 20 个字符或 20 个字节（根据字符集而定），个别字符可能需要多个字节	用户账户不能仅包括句点 (.)、空格或以句点结束。任何前导句点或空格都将被裁剪。Windows NT 4.0 及其以前版本的登录格式 (DomainName\UserName) 不支持使用 @ 符号。Windows 2000 登录名称对域是唯一的，而 Windows Server 2003/2008 登录名称在林内是唯一的。
计算机账户	NetBIOS = 15 个字符或 15 个字节（依赖于字符集），个别字符可能需要不止一个字节。 DNS = 63 个字符或 63 个字节（依赖于字符集和完全合格的域名 (FQDN) 的 255 个字符），个别字符可能需要不止一个字节	计算机账户不能仅包含数字、句点 (.) 或空格。任何前导句点或空格都将被裁剪
组账户	依赖于字符集的 63 个字符或 63 个字节，个别字符可能需要不止一个字节	组账户不能仅包含数字、句点 (.) 或空格。任何前导句点或空格都将被裁剪

3.2 安装与删除活动目录

在 Windows 2000 Server 系统中已经有了活动目录，经过 Windows Server 2003 平台的完善，Windows Server 2008 中的活动目录服务功能更加强大，管理更加方便。不过，活动目录并不是系统默认安装组件，需要管理员手动安装后才能使用。无论在 Windows 2000/2003 系统中，还是在 Windows Server 2008 系统中都需要运行 Dcpromp.exe 命令启动安装向导并安装。

3.2.1 记录与设置服务器的相关参数

将 Windows Server 2008 的计算机升级到 Active Directory 服务器时，应首先记录计算机的相关参数，如 IP 地址和计算机名等并记录要进行的工作。

使用管理员用户账户登录到系统，通过“网络和共享中心”打开本地连接属性查看当前的 TCP/IP 地址，如图 3-8 所示。

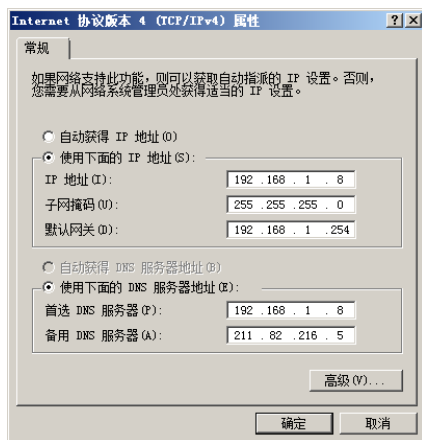


图 3-8 本地连接属性



注意：

对于将要升级到 Active Directory 服务器的计算机来说，首选的 DNS 服务器必须设置为本身的 TCP/IP 地址，并且必须是一个静态的地址。



3.2.2 安装域控制器和活动目录

在 Windows 2000/2003 系统中，可以直接运行 dcpromo 命令来启动“Active Directory 安装向导”，从而安装活动目录。而将 Windows Server 2008 升级为域控制器时，必须首先安装 Active Directory 域服务，然后运行 dcpromo 命令安装活动目录。

1. 安装 Active Directory 域服务

① 在“初始配置任务”窗口中单击“添加角色”超级链接，运行“添加角色向导”。当显示如图 3-9 所示的“选择服务器角色”对话框时，在“角色”列表框中选中“Active Directory 域服务”复选框。

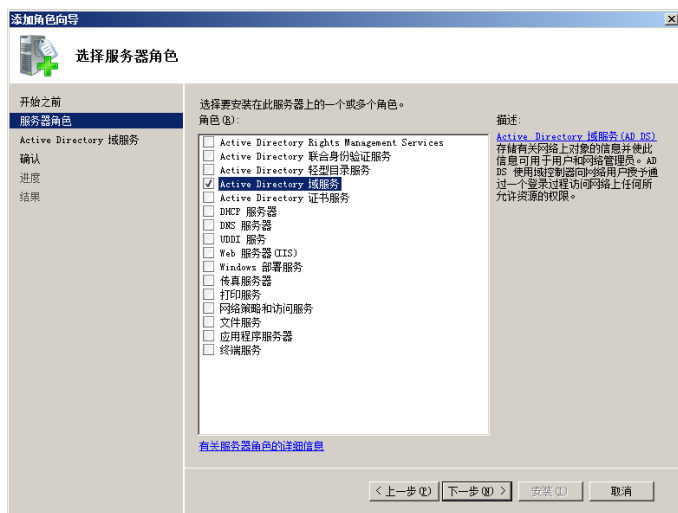


图 3-9 “选择服务器角色”对话框

② 单击“下一步”按钮，显示如图 3-10 所示的“Active Directory 域服务”对话框，其中简要介绍了域服务的作用及注意事项。

③ 单击“下一步”按钮，显示如图 3-11 所示的“确认安装选择”对话框，要求确认要安装的服务。



图 3-10 “Active Directory 域服务”对话框



图 3-11 “确认安装选择”对话框

④ 单击“安装”按钮，开始安装域服务。安装完成后，显示如图 3-12 所示的“安装结果”对话框，提示域服务已安装成功。

⑤ 单击“关闭”按钮，返回“服务器管理器”窗口。展开“角色”，即可看到 Active Directory 域服务已安装，其中提示需运行 dcpromo.exe 来安装域控制器，如图 3-13 所示。



图 3-12 “安装结果”对话框

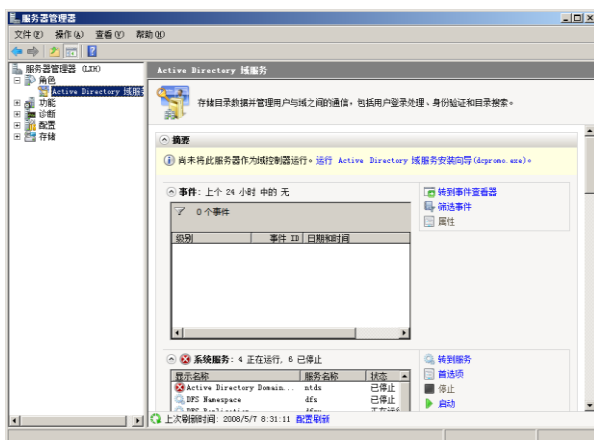


图 3-13 提示需运行 dcpromo.exe 来安装域控制器

2. 安装活动目录

① 单击“开始”→“运行”选项，运行 dcpromo.exe 命令。打开“Active Directory 域服务安装向导”对话框，如图 3-14 所示。

② 单击“下一步”按钮，显示如图 3-15 所示的“操作系统兼容性”对话框。

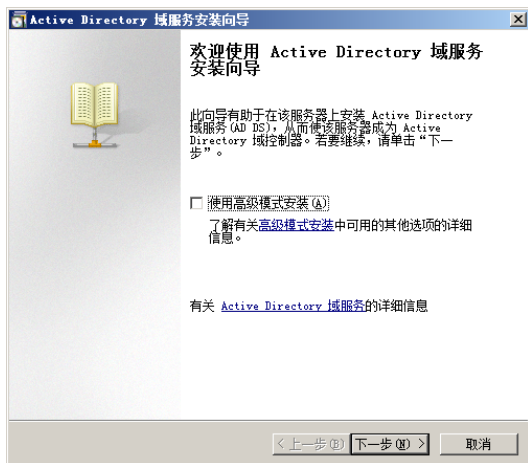


图 3-14 “Active Directory 域服务安装向导”对话框

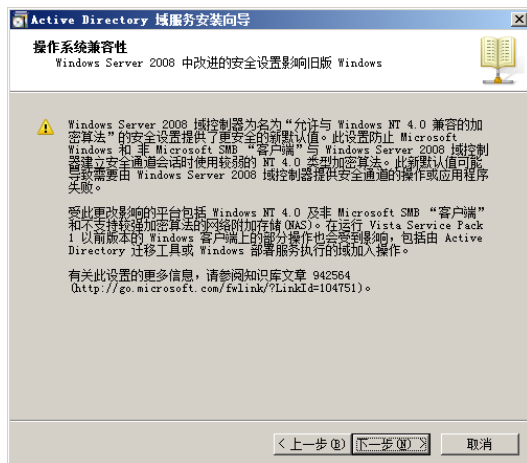


图 3-15 “操作系统兼容性”对话框

③ 单击“下一步”按钮，显示如图 3-16 所示的“选择某一部署配置”对话框。由于这是第 1 台域控制器，因此选择“在新林中新建域”单选按钮。

④ 单击“下一步”按钮，显示如图 3-17 所示的“命名林根域”对话框。在“目录林根级域的 FQDN”文本框中输入事先准备好的 DNS 域名，如 coolpen.net。

⑤ 单击“下一步”按钮，开始检查该域名及其相应的 NetBIOS 名是否已在网络中使用。完成后显示如图 3-18 所示的“设置林功能级别”对话框，其中提供了 3 种模式，即 Windows 2000、Windows Server 2003 和 Windows Server 2008，可根据网络中存在的最低 Windows 版本的域控制器来选择。

⑥ 单击“下一步”按钮，显示如图 3-19 所示的“设置域功能级别”对话框。根据网络中存在的 Windows Server 版本，在“域功能级别”下拉列表框中选择相应的域功能级别。



图 3-16 “选择某一部署配置”对话框

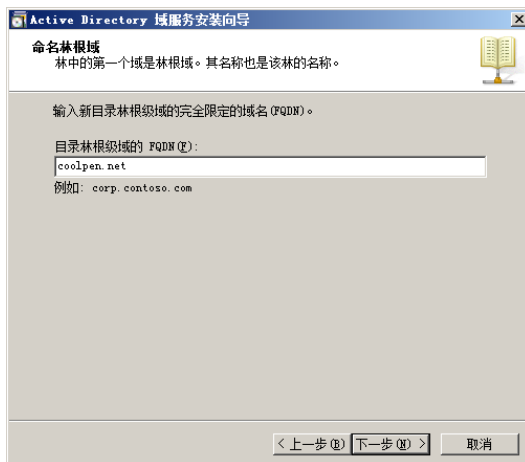


图 3-17 “命名林根域”对话框

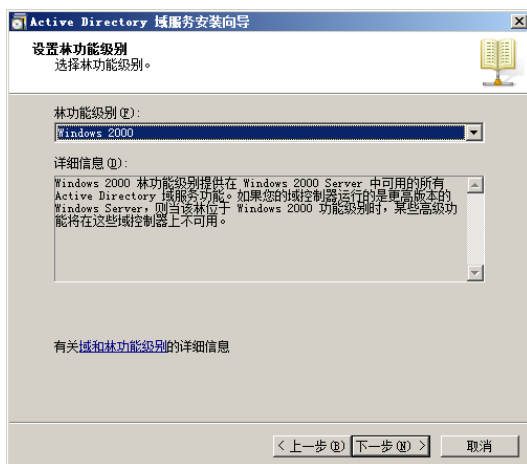


图 3-18 “设置林功能级别”对话框

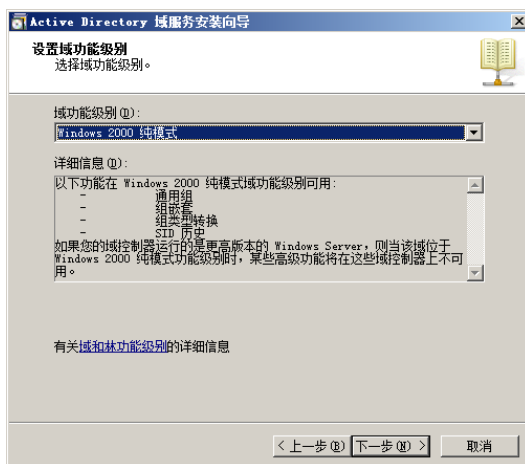


图 3-19 “设置域功能级别”对话框

⑦ 单击“下一步”按钮，开始检查 DNS 配置。完成后显示如图 3-20 所示的“其他域控制器选项”对话框，选中“DNS 服务器”复选框。

⑧ 单击“下一步”按钮，开始检查 DNS 配置。并显示如图 3-21 所示的警告框，提示没有找到父域。

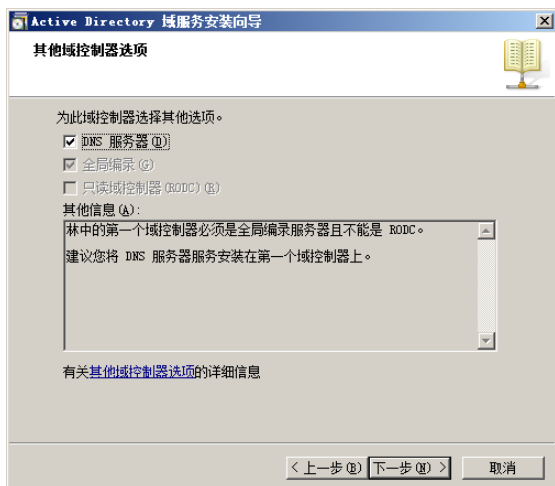


图 3-20 “其他域控制器选项”对话框

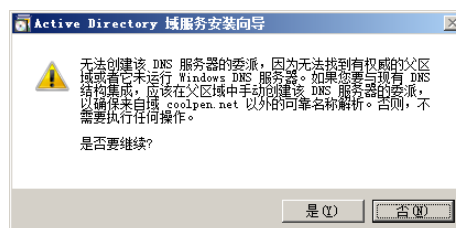


图 3-21 警告框

⑨ 单击“是”按钮，显示如图 3-22 所示的“数据库、日志文件和 SYSVOL 的位置”对话框。为了提高系统性能，并便于日后出现故障时恢复，建议将数据库和日志文件夹指定为非系统分区。

⑩ 单击“下一步”按钮，显示如图 3-23 所示的“目录服务还原模式的 Administrator 密码”对话框，在其中设置还原目录服务时的密码。

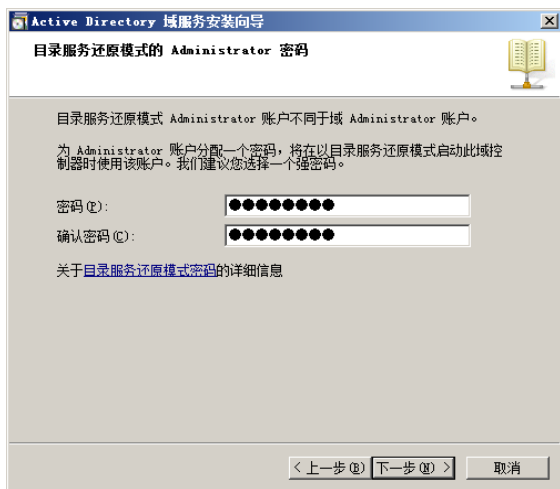
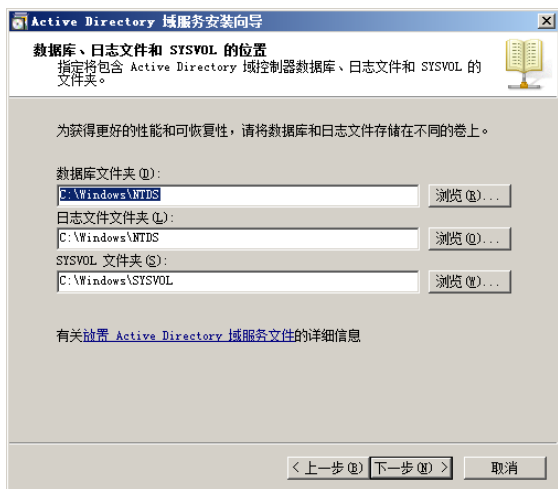


图 3-22 “数据库、日志文件和 SYSVOL 的位置”对话框 图 3-23 “目录服务还原模式的 Administrator 密码”对话框

⑪ 单击“下一步”按钮，显示如图 3-24 所示的“摘要”对话框，其中列出前面所做的配置信息。如果需要更改，则单击“上一步”按钮返回。

⑫ 单击“下一步”按钮，安装向导开始配置域服务，如图 3-25 所示。由于此过程可能需要几分钟到几小时，因此如果不想等待，也可选中“完成后重新启动”复选框，安装完成后由系统自动重新启动。

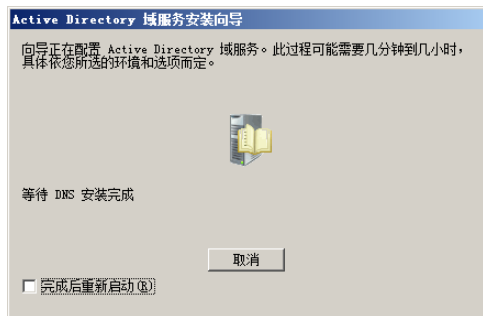
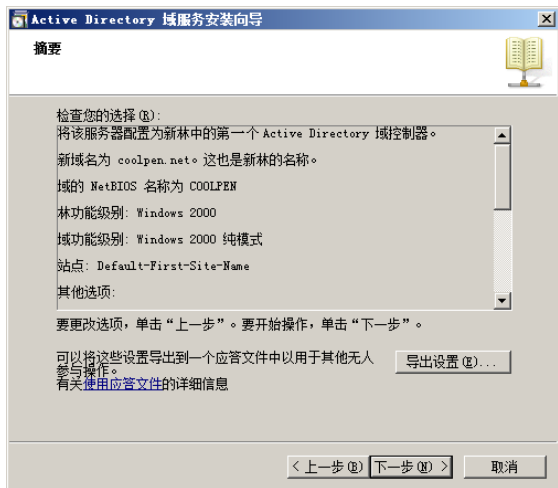


图 3-24 “摘要”对话框

图 3-25 开始配置域服务

⑬ 配置完成后，显示如图 3-26 所示的“完成 Active Directory 域服务安装向导”对话框，提示 Active Directory 域服务安装完成。

⑭ 单击“完成”按钮，显示如图 3-27 所示的提示框，提示必须重新启动计算机才能使更改生效。

⑮ 单击“立即重新启动”按钮，重新启动计算机。当重启后登录域时，用户账户需使用“域名\账户名”的格式登录，如图 3-28 所示。

⑩ 登录到系统以后，单击“开始”→“管理工具”→“Active Directory 用户和计算机”选项。显示如图 3-29 所示的“Active Directory 用户和计算机”窗口，在其中可管理域中的所有用户账户。



图 3-26 “完成 Active Directory 域服务安装向导”对话框



图 3-27 提示重新启动



图 3-28 登录域

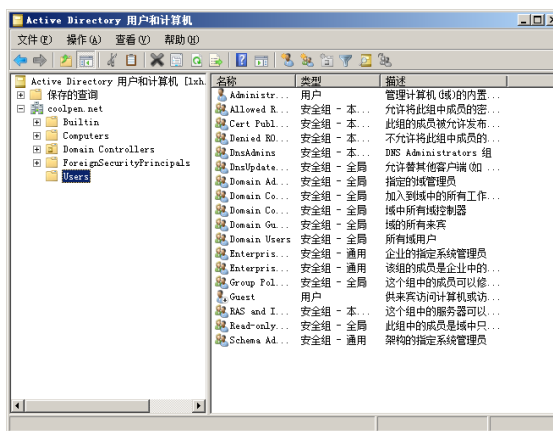


图 3-29 “Active Directory 用户和计算机”窗口

至此，活动目录安装完成。

3.2.3 创建子域

在创建子域之前，应把子域服务器的 DNS 服务器地址设置为主域控制器的 IP 地址。这里主域名为“coolpen.net”，待设置的子域域名为“book.coolpen.net”。安装过程如下。

① 运行 dcpromo 命令，显示如图 3-30 所示的提示框。安装程序会检测系统，并自动安装 Active Directory 域服务所需的文件。

② 安装完成后，启动“Active Directory 域服务安装向导”。连续单击“下一步”按钮，当显示如图 3-31 所示的“选择某一部署配置”对话框时选择“现在林”和“在现有林中新建域”单选按钮。

③ 单击“下一步”按钮，显示如图 3-32 所示的“网络凭据”对话框。在“输入位于计划安装此域控制器的林中任何域的名称”文本框中输入网络中已安装的域名称，如 coolpen.net。

④ 单击“设置”按钮，显示如图 3-33 所示的“Windows 安全”对话框，输入具有加入域权限的用户账户和密码。



图 3-30 检测系统并安装 Active Directory 域服务所需的文件



图 3-31 “选择某一部署配置”对话框



图 3-32 “网络凭据”对话框

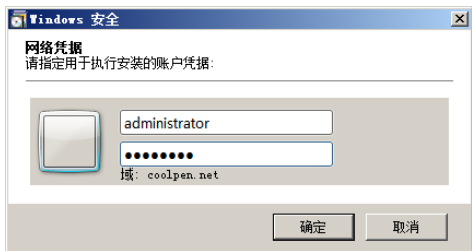


图 3-33 “Windows 安全”对话框

- ⑤ 单击“确定”按钮，添加到“备用凭据”列表框中，如图 3-34 所示。
- ⑥ 单击“下一步”按钮，开始检测域，并显示如图 3-35 所示的“命名新域”对话框。在“父域的 FQDN”文本框中输入主域的域名，或单击“浏览”按钮选择。在“子域的单标签 DNS 名称”文本框中输入子域的 DNS 名称，如 book。



图 3-34 添加到“备用凭据”列表框中

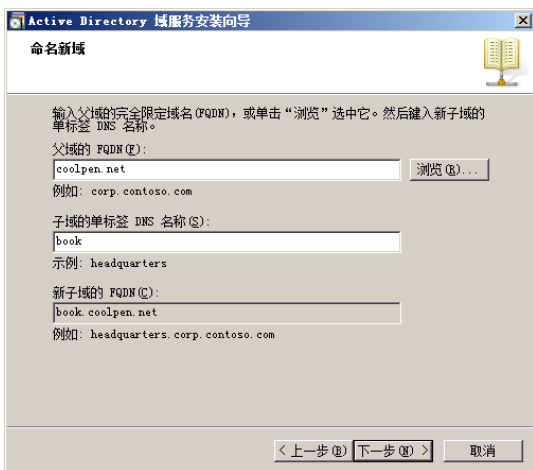


图 3-35 “命名新域”对话框

⑦ 单击“下一步”按钮，开始验证 DNS 名与 NetBIOS 名称，完成后显示如图 3-36 所示的“设置域功能级别”对话框。根据网络中存在的 Windows Server 版本，在“域功能级别”下拉列表框中选择相应的域功能级别。

⑧ 单击“下一步”按钮，显示如图 3-37 所示的“请选择一个站点”对话框，在“站点”列表框中为新域控制器选择站点。

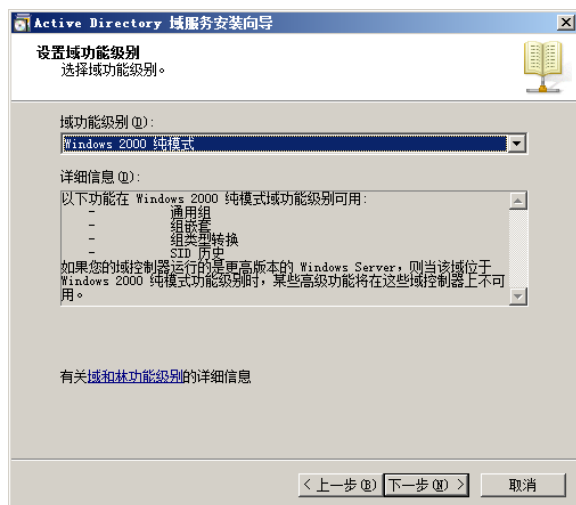


图 3-36 “设置域功能级别”对话框



图 3-37 “请选择一个站点”对话框

⑨ 单击“下一步”按钮，显示如图 3-38 所示的“其他域控制器选项”对话框，选中“DNS 服务器”复选框。如果要子域控制器安装为全局编录服务器，可选中“全局编录”复选框。

⑩ 单击“下一步”按钮，完成设置数据库、日志文件和 SYSVOL 的位置，并设置目录服务还原模式的 Administrator 密码等操作。然后开始安装并配置 Active Directory 域服务，如图 3-39 所示。

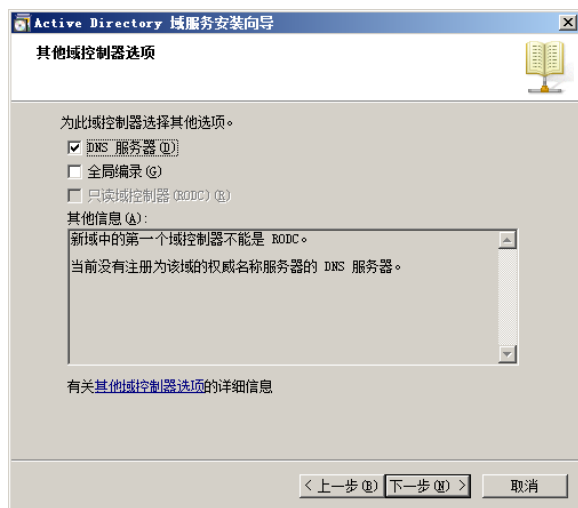


图 3-38 “其他域控制器选项”对话框

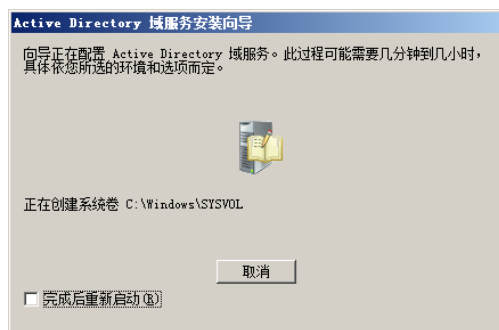


图 3-39 安装并配置 Active Directory 域服务

⑪ 配置完成以后，显示如图 3-40 所示的对话框，提示安装完成的 Active Directory 域服务。

⑫ 单击“完成”按钮，根据系统提示重新启动服务器，即可登录到该子域控制器。

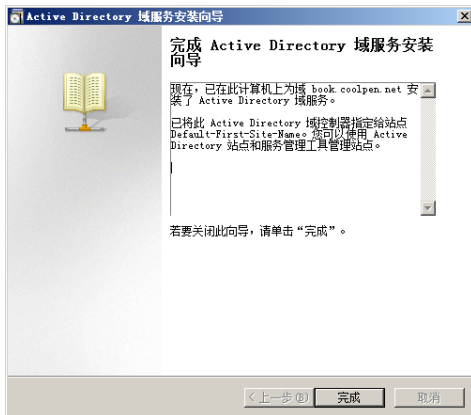


图 3-40 安装完成的 Active Directory 域服务

3.2.4 删除 Active Directory

如果网络中不再需要使用域控制器，或者需将域控制器用做其他服务器，即可将 Active Directory 删除。并降级为独立服务器或成员服务器，而不必重新安装系统。不过在删除活动目录之前，需要注意以下事项。

- (1) 如果该域内还有其他域控制器，则该域会被降级为该域的成员服务器。
- (2) 如果这个域控制器是该域的最后一个域控制器，则被降级后，由于该域内将不存在任何域控制器，因此该域控制器会被删除，而该计算机也会被降级为独立服务器。
- (3) 如果这台域控制器是“全局编录”服务器，则降级后，它将不再担当“全局编录”的角色。因此应首先确定网络中是否还有其他“全局编录”。如果没有，应首先另外指派一台域控制器来担任“全局编录”；否则将影响用户的登录。指派时可以单击“开始”→“管理工具”→“Active Directory 站点和服务”→“Sites”→“Default-First-Site-Name”→“Servers”选项，选择要扮演“全局编录”角色的服务器名称。右击“NTDS Settings”并选择快捷菜单中的“属性”选项，在显示的“NTDS Settings 属性”对话框中选中“全局编录”复选框。

删除 Active Directory 的操作步骤如下。

- ① 运行 `dcpromo` 命令，启动“Active Directory 域服务安装向导”。如果域控制器是全局编录服务器，在欢迎界面中单击“下一步”按钮时会显示如图 3-41 所示的提示框，提示该域控制器是全局编录服务器。
- ② 单击“确定”按钮，显示如图 3-42 所示的“删除域”对话框，选中“删除该域，因为此服务器是该域中的最后一个域控制器”复选框。

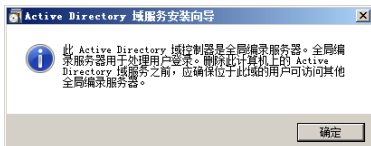


图 3-41 提示域控制器是全局编录服务器

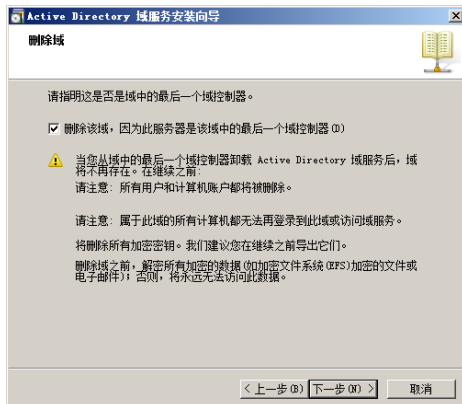


图 3-42 “删除域”对话框

③ 单击“下一步”按钮，显示如图 3-43 所示的“应用程序目录分区”对话框，提示将保留此列表框中的应用程序目录分区的最后副本。

④ 单击“下一步”按钮，显示如图 3-44 所示的“确认删除”对话框，选中“删除该 Active Directory 域控制器上的所有应用程序目录分区”复选框。

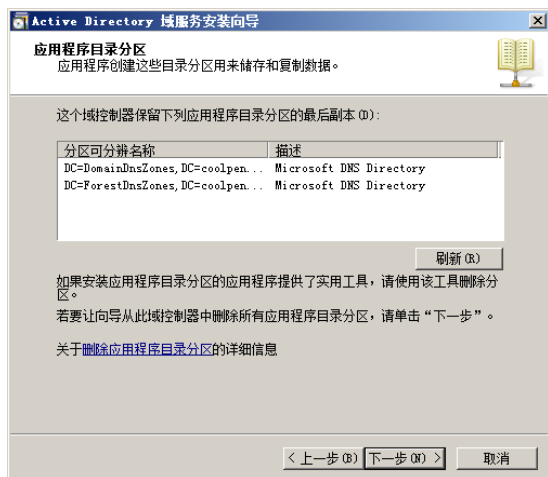


图 3-43 “应用程序目录分区”对话框

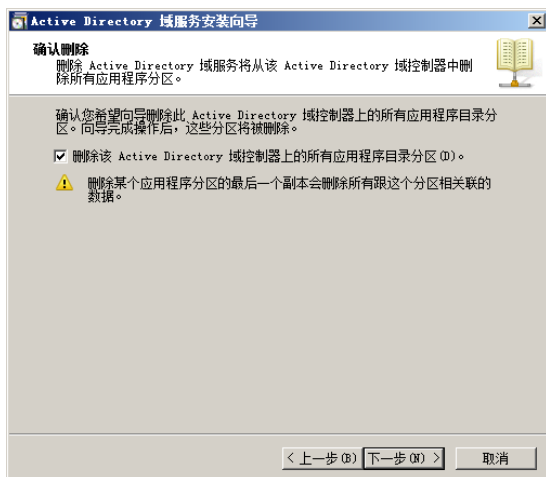


图 3-44 “确认删除”对话框

提示 如果网络中还存在有其他域控制器，就会显示如图 3-45 所示的提示框，要求确认是否是最后一个域控制器。

⑤ 单击“是”按钮，显示如图 3-46 所示的“Administrator 密码”对话框，在“密码”和“确认密码”文本框中输入 Administrator 账户的密码。



图 3-45 提示框

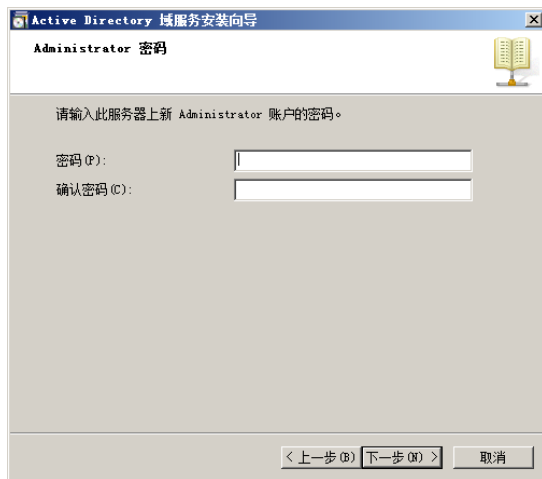


图 3-46 “Administrator 密码”对话框

⑥ 单击“下一步”按钮，显示如图 3-47 所示的“摘要”对话框，提示删除完成后此域将不再存在。

⑦ 单击“下一步”按钮，开始配置 Active Directory 服务并删除域控制器。完成后显示如图 3-48 所示的对话框，提示域控制器已删除。

⑧ 单击“完成”按钮，根据系统提示重新启动计算机，该域控制器即成为独立服务器。

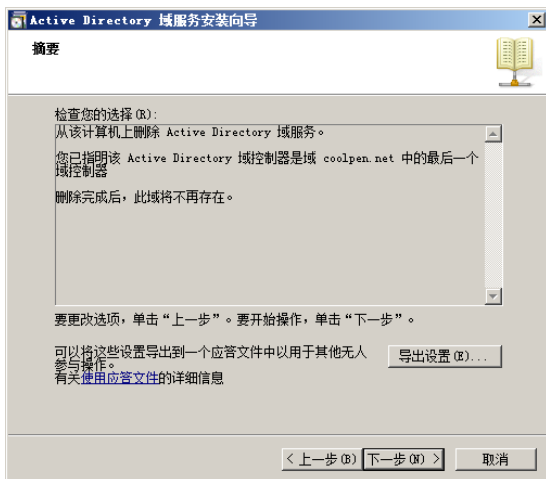


图 3-47 “摘要”对话框



图 3-48 提示域服务已删除

3.2.5 创建辅助域控制器

为了保证网络正常稳定地运行，避免域控制器出现故障而导致用户不能登录，通常会在网络中再安装一个附加的域控制器。即辅助域控制器，也称为“辅助域控制器”。当主域控制器出现故障时，辅助控制器能接管主域控制器的工作。继续为网络提供服务，维护网络的正常运行，同时还可以起到备份数据的作用。

在安装之前，应把辅助域控制器的 DNS 服务器地址设置为主域控制器的 IP 地址；否则可能无法找到主域。安装过程如下。

① 运行 `dcpromo` 命令，安装程序会检测并自动安装 Active Directory 域服务所需的文件，然后启动“Active Directory 域服务安装向导”。

② 连续单击“下一步”按钮，当显示“选择某一部署配置”对话框时选择“现在林”及“向现有域添加域控制器”单选按钮，如图 3-49 所示。

③ 单击“下一步”按钮，显示如图 3-50 所示的“网络凭据”对话框，在“输入位于计划安装此域控制器的林中任何域的名称”文本框中输入网络中已安装的域名称。单击“设置”按钮，添加具有加入域权限的用户账户和密码。



图 3-49 “选择某一部署配置”对话框



图 3-50 “网络凭据”对话框

④ 单击“下一步”按钮，显示如图 3-51 所示的“选择一个域”对话框，在“域”列表框中选择域。

⑤ 单击“下一步”按钮，显示如图 3-52 所示的“请选择一个站点”对话框，在“站点”列表框中选择站点。



图 3-51 “选择一个域”对话框



图 3-52 “请选择一个站点”对话框

⑥ 单击“下一步”按钮，显示如图 3-53 所示的“其他域控制器选项”对话框。选中“DNS 服务器”和“全局编录”复选框，将辅助域控制器同时作为全局编录服务器。

⑦ 继续单击“下一步”按钮，设置数据库、日志文件和 SYSVOL 的位置，并设置目录服务还原模式的 Administrator 密码等操作。然后开始安装并配置 Active Directory 域服务，如图 3-54 所示。

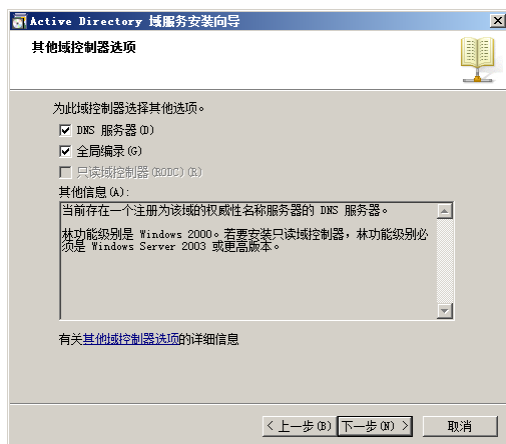


图 3-53 “其他域控制器选项”对话框



图 3-54 配置 Active Directory 域服务

⑧ 配置完成以后，显示如图 3-55 所示的“完成 Active Directory 域服务安装向导”对话框，辅助域控制器安装完成。



图 3-55 辅助域服务器安装完成

- ⑨ 单击“完成”按钮，根据系统提示重新启动计算机，并使用域用户账户登录到域。

辅助域控制器安装完成以后，客户端计算机的 DNS 服务器也要添加辅助域控制器的 IP 地址；否则无法联系辅助域控制器并获取相应信息。

3.3 备份与恢复活动目录

虽然服务器都采用了高配置的硬件设备，以及 RAID 等硬盘冗余技术，但仍难以避免因自然灾害或人为灾难而造成服务器故障，从而造成数据丢失。为了避免这种情况，应当定期备份服务器，以便在数据丢失时可以及时恢复。

3.3.1 备份系统状态

和 Windows 2000/2003 系统不同，Windows Server 2008 中没有安装“备份还原向导”，而是使用功能更加强大的“Windows Server Backup 功能”。用其可以设置备份计划，使系统在每天的特定时间自动备份，不需人为干预。不过由于所备份的数据需存储在其他存储设备中，因此服务器需要连接有外部磁盘或磁带机，或者至少安装有两块硬盘。

1. 安装 Windows Server Backup 功能

默认情况下，Windows Server Backup 功能并没有安装在 Windows Server 2008 系统中，需要由管理员手动安装。

- ① 在“初始配置任务”窗口中单击“添加功能”超级链接，运行“添加功能向导”。在“功能”列表框中选中“Windows Server Backup 功能”复选框，如图 3-56 所示。

- ② 单击“下一步”按钮，显示如图 3-57 所示的“确认安装选择”对话框，其中列出已选择的功能。



图 3-56 选中“Windows Server Backup 功能”复选框

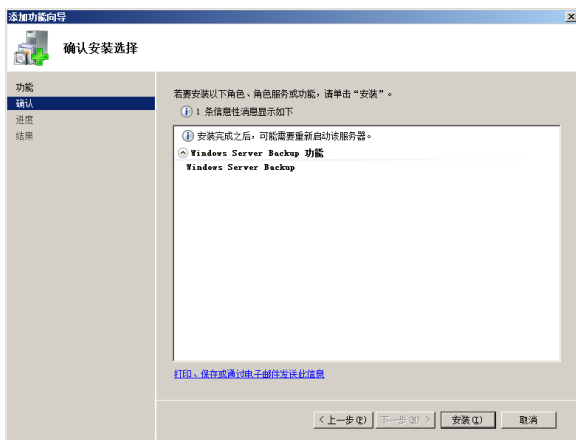


图 3-57 “确认安装选择”对话框

- ③ 单击“安装”按钮，开始安装所选功能。安装完成后显示如图 3-58 所示的“安装结果”对话框，提示 Windows Server Backup 功能安装成功。

- ④ 单击“关闭”按钮关闭向导，打开“服务器管理器”窗口。在“功能”窗格中即可看到 Windows Server Backup 功能已被安装，如图 3-59 所示。

2. 备份计划

为了提高工作效率，可以设置备份计划。即让服务器在事先设定的时间自动运行备份程序，从而为网络管理员节省时间和精力。

- ① 在“服务器管理器”窗口中依次展开“存储”→“Windows Server Backup”选项，如图 3-60 所示，此时尚未配置任何备份。

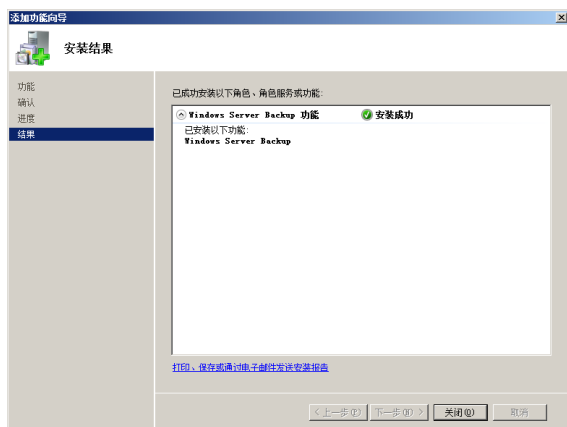


图 3-58 “安装结果”对话框



图 3-59 已安装的功能

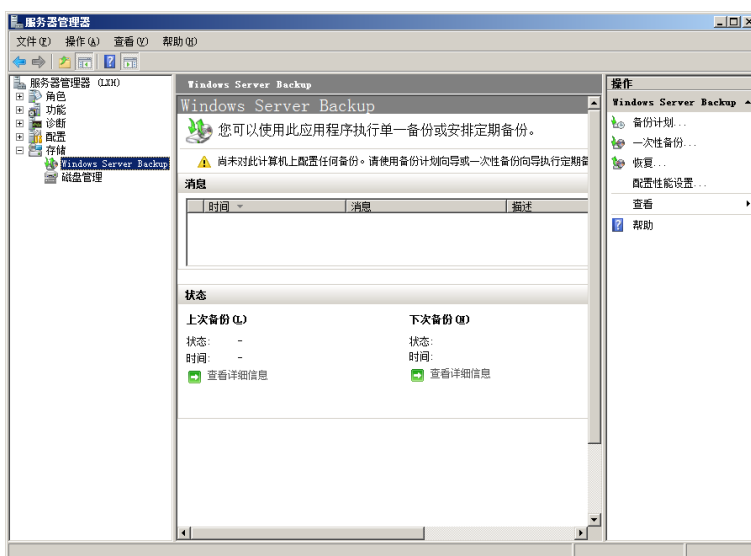


图 3-60 “Windows Server Backup”选项

② 在窗口右侧的“操作”列表中单击“备份计划”超级链接，运行“备份计划向导”，如图 3-61 所示。

③ 单击“下一步”按钮，显示如图 3-62 所示的“选择备份配置”对话框。如果要备份该服务器中所有的数据、应用程序和系统状态，则选择“整个服务器（推荐）”单选按钮，这里选择该单选按钮；如果要选择所备份的分区，则选择“自定义”单选按钮。

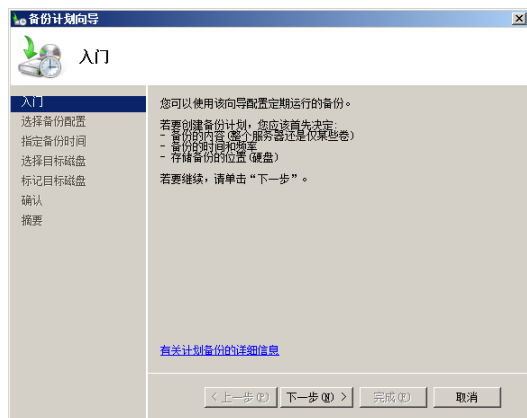


图 3-61 备份计划向导



图 3-62 “选择备份配置”对话框

④ 单击“下一步”按钮，显示如图 3-63 所示的“指定备份时间”对话框。如果要每天备份一次，则选择“每日一次”单选按钮，并在“选择时间”下拉列表框中选择备份时间，建议选择在夜间或凌晨不使用服务器的时间。对于重要的应用，则可选择“每日多次”单选按钮，并选择在每天的哪些时间备份。

⑤ 单击“下一步”按钮，显示如图 3-64 所示的“选择目标磁盘”对话框，在“可用磁盘”中可以选择用于存储备份的磁盘。

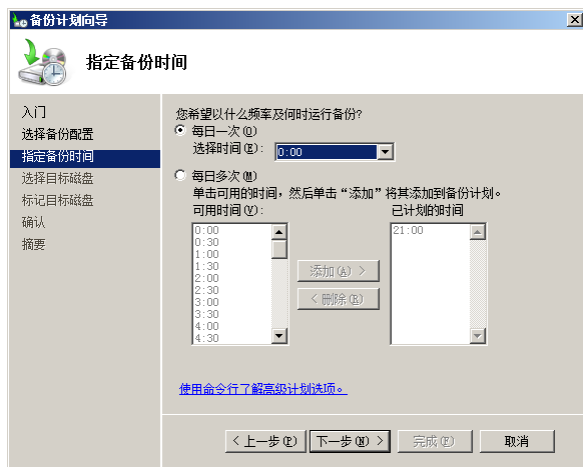


图 3-63 “指定备份时间”对话框



图 3-64 “选择目标磁盘”对话框



提示

如果没有外接磁盘或磁带机，而服务器上安装的硬盘不会显示在“可用磁盘”列表中，可单击“显示所有可用磁盘”按钮选择本地服务器中的硬盘。

⑥ 单击“下一步”按钮，显示如图 3-65 所示的警告框，提示将重新格式化所选磁盘。该磁盘中的所有卷和数据都将被删除，并且将不显示在 Windows 资源管理器中。

⑦ 单击“是”按钮，显示如图 3-66 所示的“标记目标磁盘”对话框，提示将使用列表中的信息标记该磁盘。

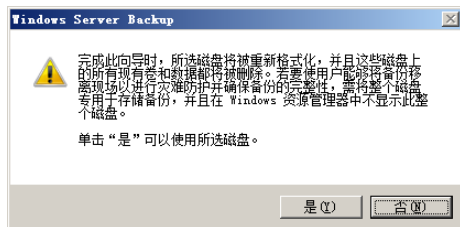


图 3-65 警告框

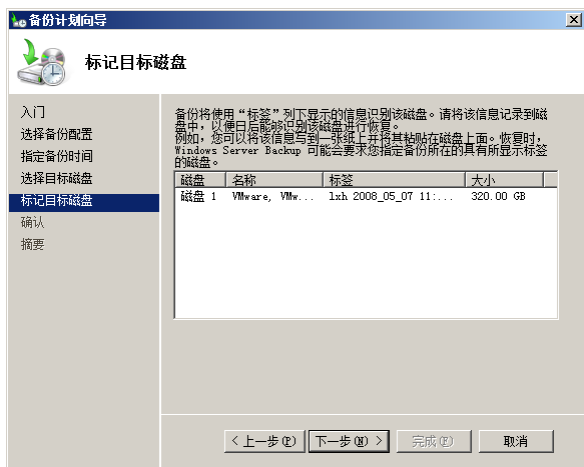
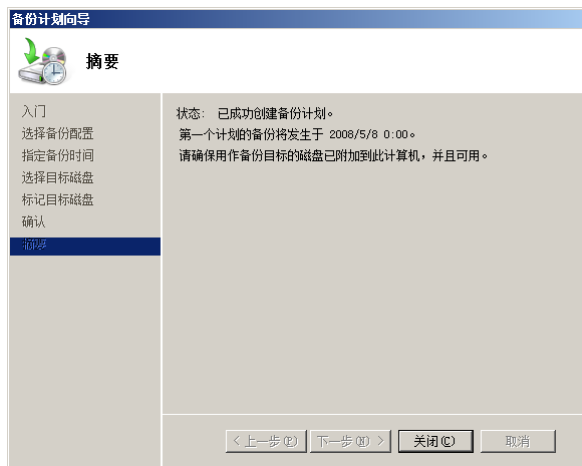


图 3-66 “标记目标磁盘”对话框

⑧ 单击“下一步”按钮，显示如图 3-67 所示的“确认”对话框，其中列出所做的设置。如需更改，则单击“上一步”按钮返回。

⑨ 单击“完成”按钮，开始格式化磁盘。完成后显示如图 3-68 所示的“摘要”对话框，备份计划创建完成，单击“关闭”按钮关闭即可。



备份计划创建完成以后，系统就会根据计划在每天的计划时间开始备份服务器，而在 Windows 资源管理器中将不显示存储备份的磁盘。

3. 备份数据

利用备份向导可以备份整个分区或者整个磁盘中的数据。由于活动目录安装在 C 盘，因此备份 C 盘即可备份活动目录的系统数据。

① 在“Windows Server Backup”窗口右侧的“操作”列表中单击“一次性备份”超级链接，显示如图 3-69 所示的“备份选项”对话框，选择“不同选项”单选按钮。

② 单击“下一步”按钮，显示如图 3-70 所示的“选择备份配置”对话框。选择要备份的类型，这里选择“自定义”单选按钮。



③ 单击“下一步”按钮，显示如图 3-71 所示的“选择备份项目”对话框。在列表框中选择欲备份的分区，由于活动目录安装在 C 盘，因此这里选择 C 分区。

④ 单击“下一步”按钮，显示如图 3-72 所示的“指定目标类型”对话框。选择存储备份文件的位置，可以存储在本地磁盘的非系统分区或网络中的远程共享文件夹中。

⑤ 单击“下一步”按钮，显示如图 3-73 所示的“选择备份目标”对话框。由于选择保存在本地磁盘，因此需在“备份目标”下拉列表框中选择要存储的分区。

⑥ 单击“下一步”按钮，显示如图 3-74 所示的“指定高级选项”对话框，选择要创建的卷影复

制服务备份的类型。如果使用第三方的备份软件，可选择“VSS 副本备份”单选按钮；如果使用 Windows Server 2008 提供的备份程序，建议选择“VSS 完全备份”单选按钮。



图 3-71 “选择备份项目”对话框



图 3-72 “指定目标类型”对话框

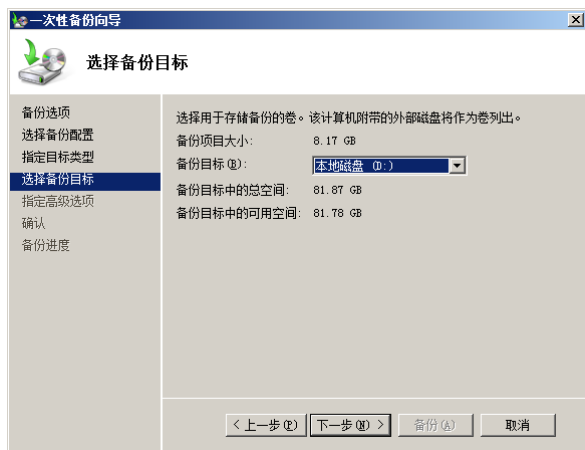


图 3-73 “选择备份目标”对话框

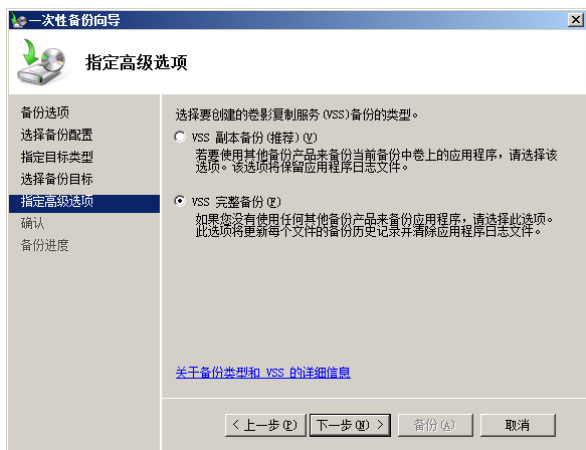


图 3-74 “指定高级选项”对话框

⑦ 单击“下一步”按钮，显示如图 3-75 所示的“确认”对话框，其中列出前面所做的配置。如果需要更改，则单击“上一步”按钮返回。

⑧ 单击“备份”按钮，开始创建卷的卷影副本。完成后开始备份，并在“项目”列表框中显示了备份进度，如图 3-76 所示。根据磁盘中的数据量，备份所需要的时间长短也不一样。

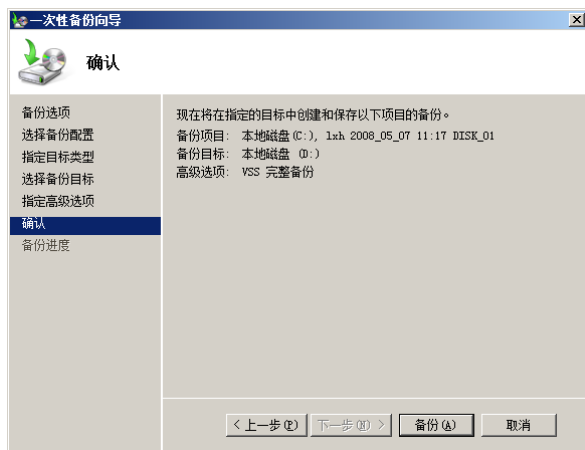


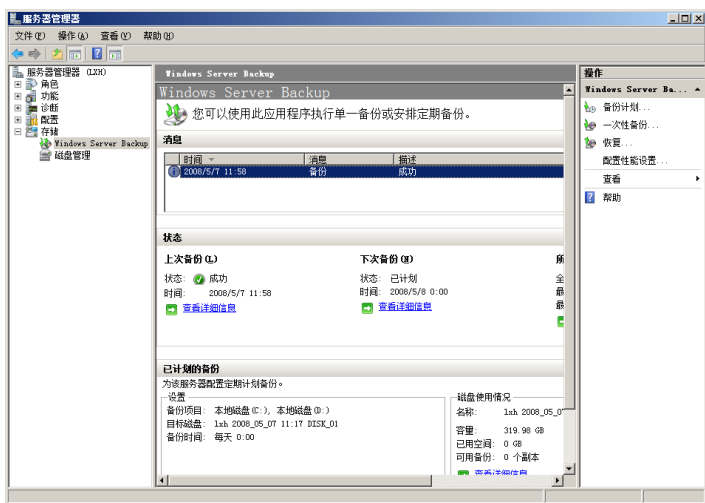
图 3-75 “确认”对话框



图 3-76 备份进度

⑨ 备份完成后，提示已完成备份，如图 3-77 所示。

⑩ 单击“关闭”按钮关闭备份向导，返回“服务器管理器”窗口，可以看到已完成的备份，如图 3-78 所示。



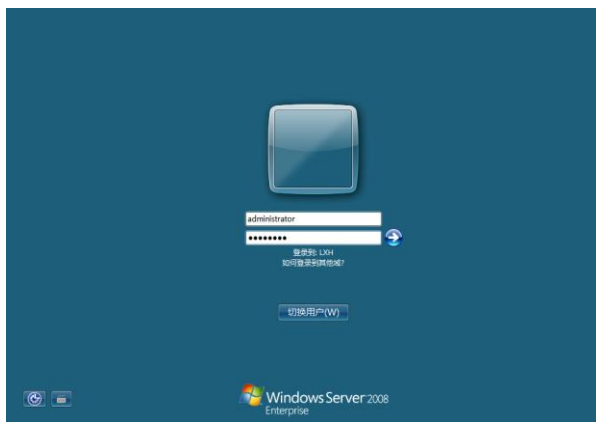
至此，活动目录备份完成。

3.3.2 恢复系统状态

当服务器出现故障时，可以利用原来的备份使用恢复向导恢复。不过，恢复操作要比备份操作复杂得多。而且为了系统安全起见，应在“目录服务还原模式”下还原。

① 重新启动系统，在进入 Windows Server 2008 启动界面前按 F8 键进入如图 3-79 所示的“高级启动选项”界面，通过键盘上的方向键选择“目录服务还原模式”选项。

② 按回车键，加载操作系统文件并启动。在登录窗口中，单击“切换用户”→“其他用户”选项。在“用户名”文本框中输入“Administrator”登录到本地计算机而不是登录到域，在“密码”文本框中输入目录还原模式密码，如图 3-80 所示。



③ 按回车键，启动到 Windows Server 2008 安全模式下的桌面，如图 3-81 所示。

④ 单击“开始”→“服务器管理器”选项，打开如图 3-82 所示的“服务器管理器”窗口，展开“存储”→“Windows Server Backup”。

⑤ 在右侧的“操作”窗口中单击“恢复”超级链接，运行“恢复向导”。在“入门”对话框中选

择“此服务器”单选按钮，如图 3-83 所示。

⑥ 单击“下一步”按钮，显示如图 3-84 所示的“选择备份日期”对话框，根据日期选择可用的备份。

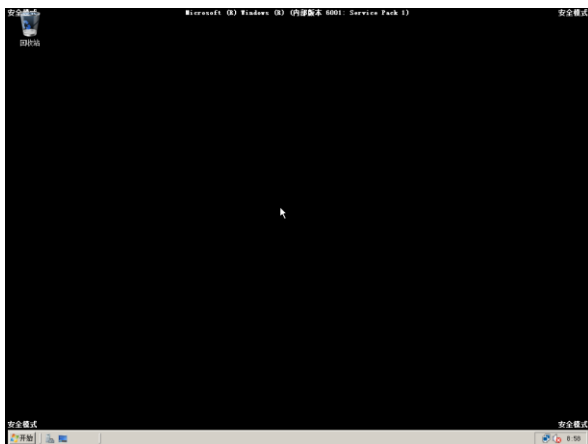


图 3-81 安全模式下的桌面

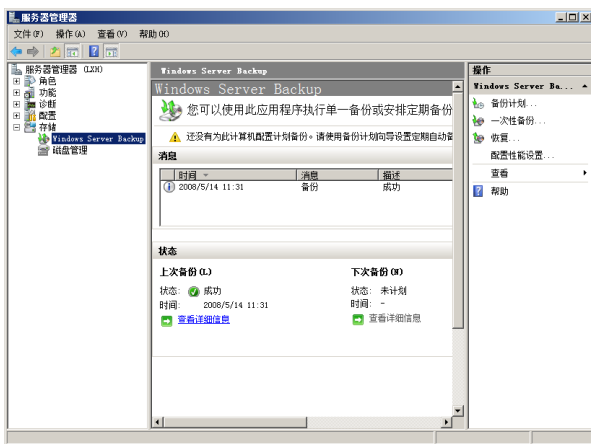


图 3-82 “服务器管理器”窗口

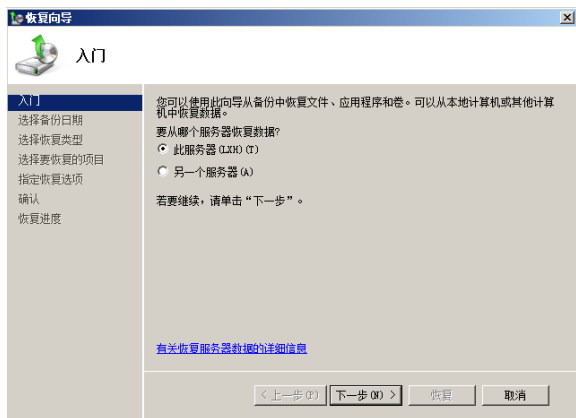


图 3-83 选择“此服务器”单选按钮



图 3-84 “选择备份日期”对话框

⑦ 单击“下一步”按钮，显示如图 3-85 所示的“选择恢复类型”对话框，选择要恢复的内容。如果选择“文件和文件夹”单选按钮，可选择要恢复文件和文件夹，这里选择该单选按钮；如果选择“卷”单选按钮，则可恢复整个 C 卷。

⑧ 单击“下一步”按钮，显示如图 3-86 所示的“选择要恢复的项目”对话框。选择“本地磁盘 (C:)”选项，恢复整个 C 分区中的文件和文件夹。



图 3-85 “选择恢复类型”对话框



图 3-86 “选择要恢复的项目”对话框

⑨ 单击“下一步”按钮，显示如图 3-87 所示的警告框，提示文件或文件夹将无法恢复到原始位置。

⑩ 单击“确定”按钮，显示如图 3-88 所示的“指定恢复选项”对话框。单击“浏览”按钮，选择先前备份的文件夹，并选择是否覆盖现有文件。

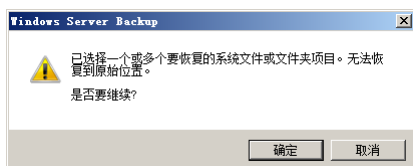


图 3-87 警告框

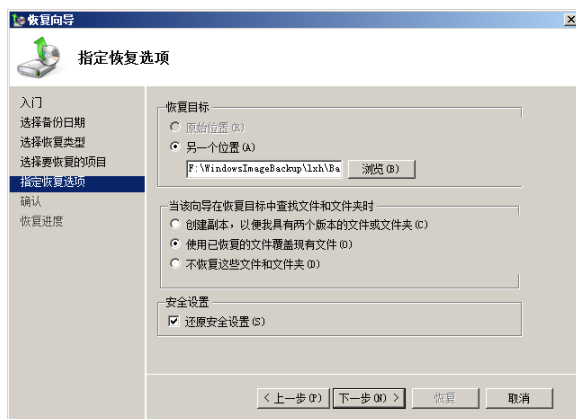


图 3-88 “指定恢复选项”对话框

⑪ 单击“下一步”按钮，显示如图 3-89 所示的“确认”对话框，在“恢复项目”列表框中显示待恢复的文件和文件夹。

⑫ 单击“恢复”按钮，显示如图 3-90 所示的“恢复进度”对话框。开始恢复文件，单击“关闭”按钮可以完成向导并继续恢复。



图 3-89 “确认”对话框



图 3-90 “恢复进度”对话框

⑬ 恢复完成以后重新启动计算机。

3.3.3 使用命令行工具

Windows Server Backup 自带命令行工具，利用 Wbadmin 命令即可备份和恢复系统数据。与向导不同，利用命令行工具可以单独备份 Active Directory 服务器的系统状态，而不是像向导一样只能备份分区或磁盘中的文件和文件夹。

1. 安装命令行工具

在安装 Windows Server Backup 时，默认没有安装命令行工具，需要管理员手动添加。

① 运行“添加功能向导”，显示“选择功能”对话框。选中“命令行工具”复选框，显示如图 3-91 所示的“添加功能向导”对话框，提示同时需要添加 Windows PowerShell 功能。



图 3-91 “添加功能向导”对话框

② 单击“添加必需的功能”按钮，选中“命令行工具”和“Windows PowerShell”复选框，如图 3-92 所示。

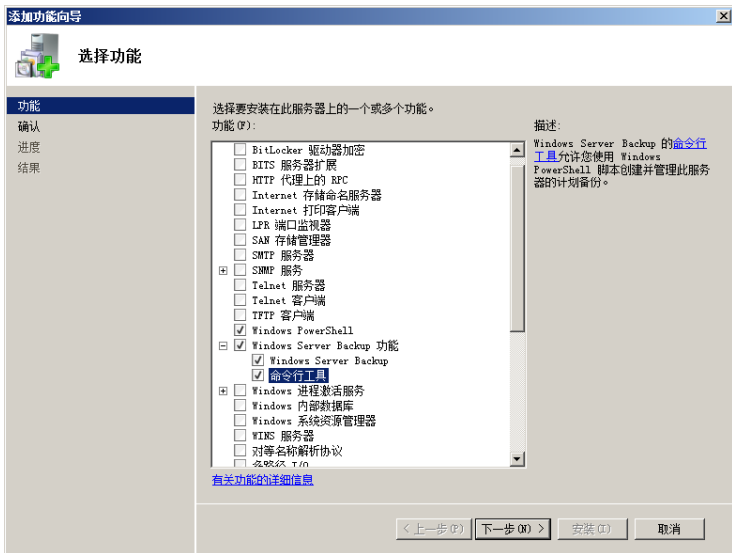


图 3-92 “选择功能”对话框

③ 单击“下一步”按钮开始安装。

2. 备份系统状态

① 单击“开始”→“命令提示符”选项，打开“命令提示符”窗口。在命令行提示符下输入“wbadmin”命令，按回车键。显示 Wbadmin 命令的帮助信息，如图 3-93 所示。

② 在命令行提示符下输入如下命令：

```
Wbadmin get disks
```

按回车键，显示服务器已经连接的磁盘，如图 3-94 所示，其中 F 盘是将用来存储备份的磁盘。

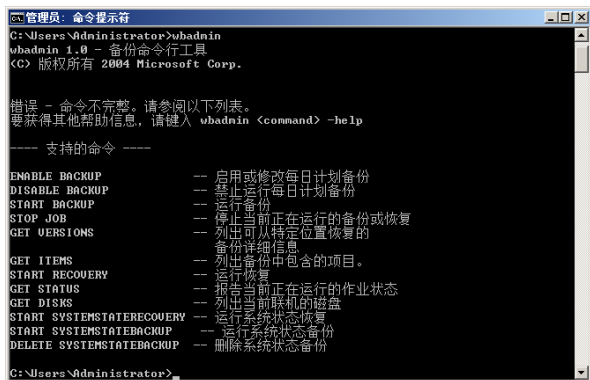


图 3-93 Wbadmin 命令帮助信息



图 3-94 已经连接的磁盘

- ③ 在命令行提示符下输入如下命令：

```
wbadmin start systemstatebackup -backuptarget:f:
```

按回车键，显示询问是否要将系统状态从 C 盘备份到 F 盘，如图 3-95 所示。

- ④ 键入 Y，按回车键创建需要备份卷的卷影副本并搜索系统状态文件，如图 3-96 所示。

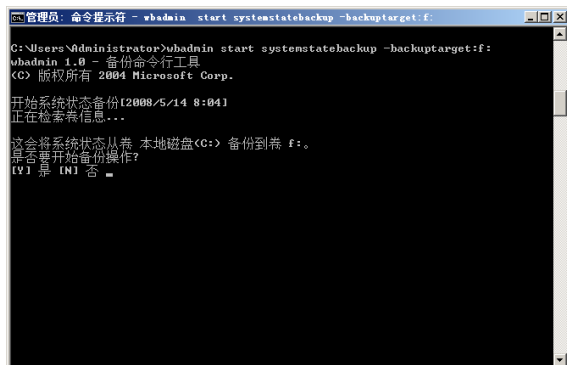


图 3-95 询问是否要将系统状态从 C 盘备份到 F 盘

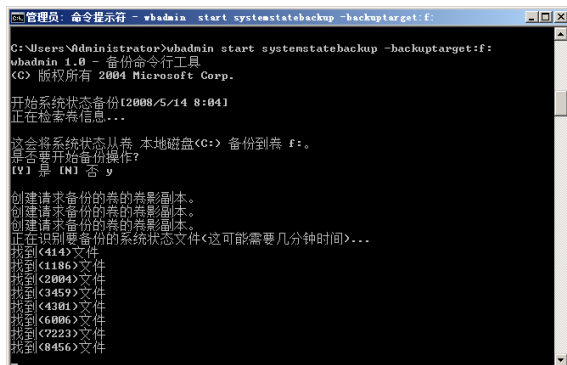


图 3-96 搜索系统状态文件

- ⑤ 搜索完成后，开始启动文件备份并显示备份进度，如图 3-97 所示。

- ⑥ 备份完成，并且创建了一个备份文件日志，如图 3-98 所示。

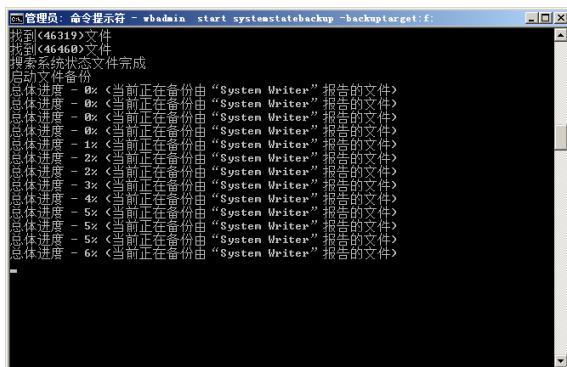


图 3-97 备份进度

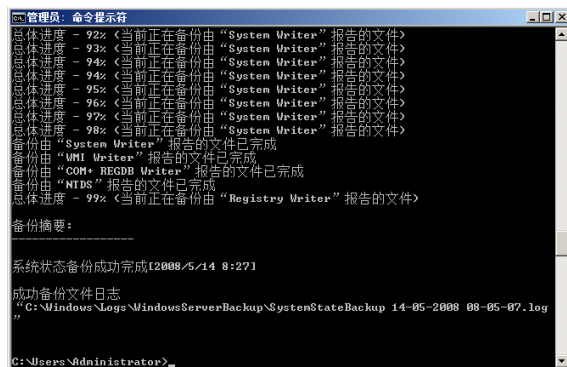


图 3-98 备份文件日志

- ⑦ 在命令行提示符下输入如下命令：

```
wbadmin get versions
```

按回车键，显示备份信息。包括备份时间、备份目标及可以恢复的组件等，如图 3-99 所示。

至此，活动目录备份完成。

3. 恢复系统状态

Windows Server Backup 采用了新的数据恢复机制，如果只是恢复文件及文件夹，可以使用恢复向导完成；如果恢复 Active Directory 数据库，则需要在目录还原模式下使用“Wbadmin.exe”完成。

- ① 重新启动系统，选择“目录还原模式”启动并登录到本地计算机。

- ② 打开“命令提示符”窗口，输入如下命令：

```
wbadmin get versions
```

按回车键，显示 Active Directory 服务器的备份列表及需要注意每次备份中的版本标识符，如图 3-100 所示。

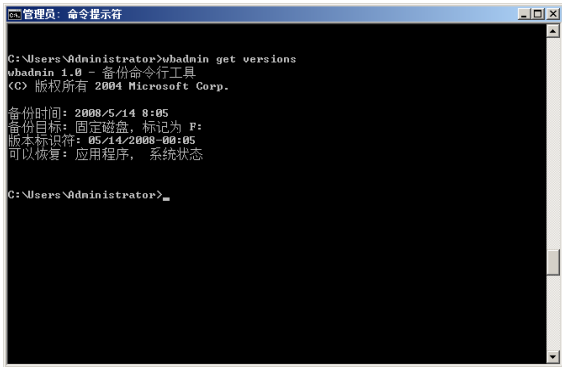


图 3-99 备份信息

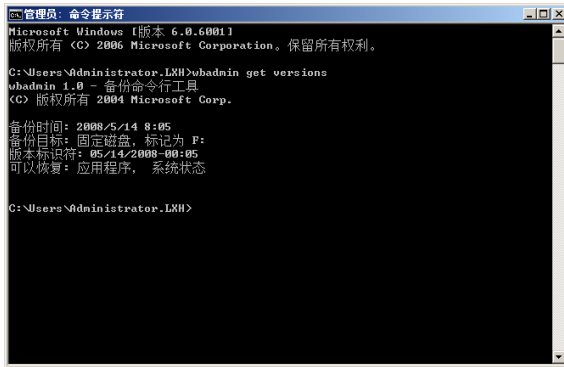


图 3-100 备份列表

- ③ 在命令行提示符下，输入如下命令：

```
wbadmin start systemstaterecovery -version:05/14/2008-00:05
```

按回车键，提示网络管理员是否要执行系统状态恢复操作，如图 3-101 所示。

- ④ 输入 Y，确认执行系统状态恢复。按回车键开始处理要还原的文件，如图 3-102 所示。



图 3-101 提示网络管理员是否要执行系统状态恢复操作



图 3-102 处理要还原的文件

- ⑤ 文件处理完成后，开始从备份还原文件并显示还原进度，如图 3-103 所示。

- ⑥ 系统状态还原完成，并创建了还原日志。同时提示需要重新启动计算机尝试恢复系统文件，如图 3-104 所示。

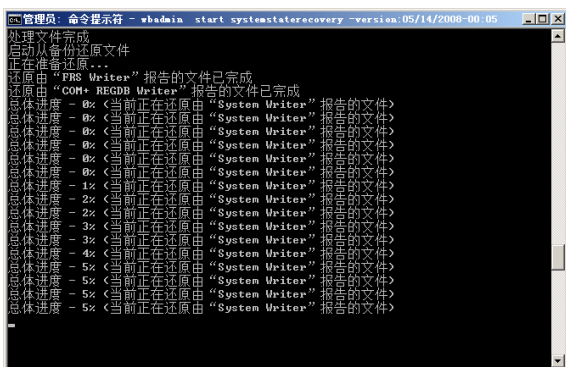


图 3-103 还原进度

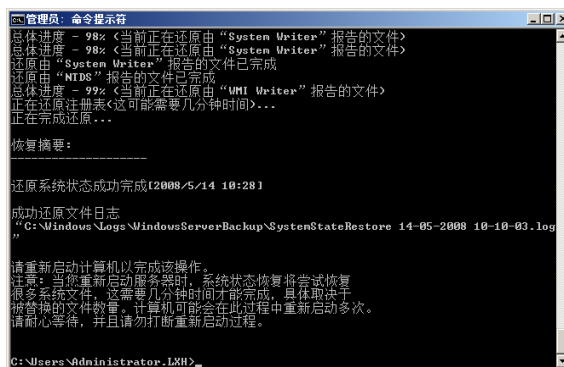


图 3-104 提示需要重新启动系统

- ⑦ 重新启动系统并登录，提示系统恢复操作已完成，如图 3-105 所示。

- ⑧ 按回车键，退出命令行工具。



图 3-105 恢复操作已完成

3.4 拯救域控制器

虽然服务器配置较高且运行比较稳定，但仍难以避免因病毒、使用或操作不当、安装添加/删除程序等原因，或者硬件故障造成操作系统出现问题。导致网络连接故障或者数据库故障，使得工作站无法正常登录到域，或者一些应用软件无法在域中安装。此时需要拯救域控制器，重新安装或者恢复域并安装或者恢复操作系统等。

3.4.1 概述

主域控制器出现故障后，可以先将辅助域控制器升级为主域控制器，然后重新安装原来的主域控制器。不过由于域控制器中保存了大量的用户及相关的信息，因此在重新安装域时必须事先备份数据，例如备份到磁带机或者活动硬盘等移动存储设备上。域控制器的故障主要有以下两种情况。

(1) 主域控制器出现故障但仍可用

如果主域控制器出现了故障，但管理员仍然可以登录。此时可以首先将数据备份到其他磁盘中并将辅助域控制器升级为主域控制器。然后在原来的主域控制器上运行 `dcpromo` 命令将其从 Active Directory 中删除，或者重新安装操作系统，再升级成主域控制器的辅助域控制器。最后将其升级成主域控制器，并恢复原来的数据。

(2) 主域控制器彻底损坏且不能恢复

如果主域控制器彻底损坏且不能恢复，此时网络将无法使用，只能将网络中的辅助域控制器升级成主域控制器。然后重新安装原来的主域控制器，升级成辅助域控制器。最后升级成主域控制器，并恢复原来的数据。

3.4.2 转移操作主机角色

如果出现故障的主域控制器还可用，转移主域控制器角色可以通过 5 个部分进行，即转移 RID 主机角色、PDC 模拟器角色、结构主机角色、域命名操作主机角色和架构主机角色；如果主域控制器已经损坏并且不可修复，只能强制占有主机角色。

1. 连接辅助域控制器

① 在主域控制器中单击“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开“Active Directory 用户和计算机”窗口。右击“Active Directory 用户和计算机”选项，在快捷菜单中选择“更改域控制器”选项，显示如图 3-106 所示的“更改目录服务器”对话框。

② 选择“此域控制器或 AD LDS 实例”单选按钮，并在可用的域控制器列表框中选择辅助域控制器。单击“确定”按钮，返回到“Active Directory 用户和计算机”窗口。

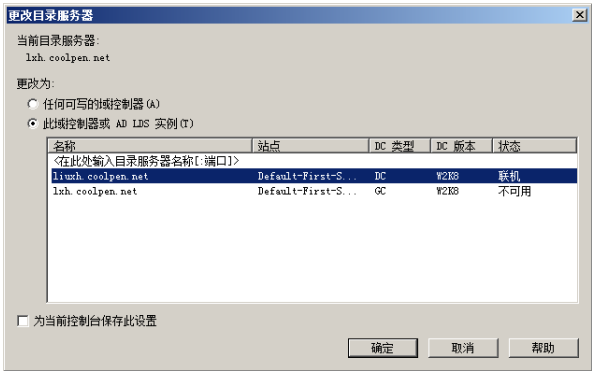


图 3-106 “更改目录服务器”对话框

2. 转移 RID 主机角色

- ① 在“Active Directory 用户和计算机”窗口中右击域控制器名“coolpen.net”选项，在快捷菜单中选择“操作主机”选项打开如图 3-107 所示的“操作主机”对话框，默认为“RID”选项卡。在“操作主机”文本框中显示的是原域控制器的计算机名，在“要传送操作主机角色到下列计算机”文本框中显示的是辅助域控制器的计算机名。
- ② 单击“更改”按钮，将更改 RID 主机角色到转移到辅助域控制器上。显示如图 3-108 所示的提示框，提示是否确定要传送操作主机角色。

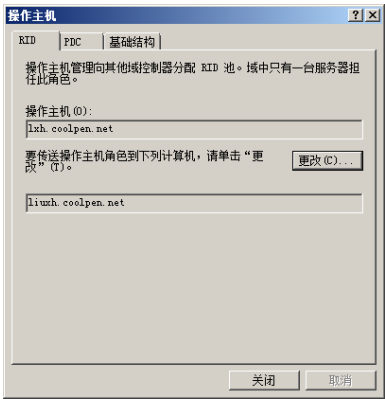


图 3-107 “操作主机”对话框

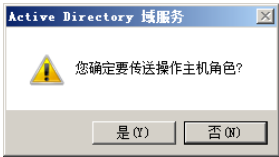


图 3-108 提示框

- ③ 单击“是”按钮，转移操作主机角色。更改完成后显示如图 3-109 所示的提示框，提示操作主机角色传送成功。
- ④ 单击“确定”按钮，返回到“操作主机”对话框，如图 3-110 所示。

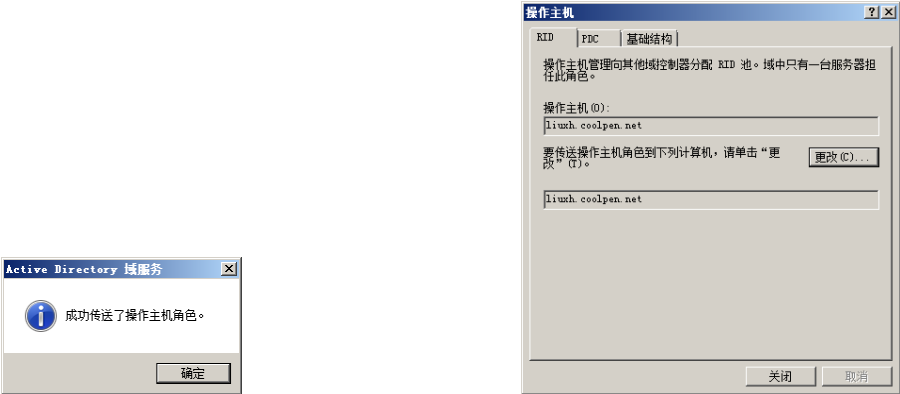


图 3-109 操作主机角色传送成功

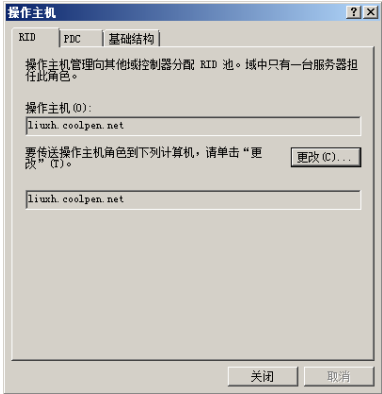


图 3-110 “操作主机”对话框

3. 转移 PDC 主机角色

- ① 切换到如图 3-111 所示的“PDC”选项卡，在“操作主机”文本框中显示的是原主域控制器的计算机名，在“要传送操作主机角色到下列计算机”文本框中显示的是辅助域控制器的计算机名。
- ② 单击“更改”按钮，将 PDC 主机由主域控制器转移到辅助域控制器，如图 3-112 所示。

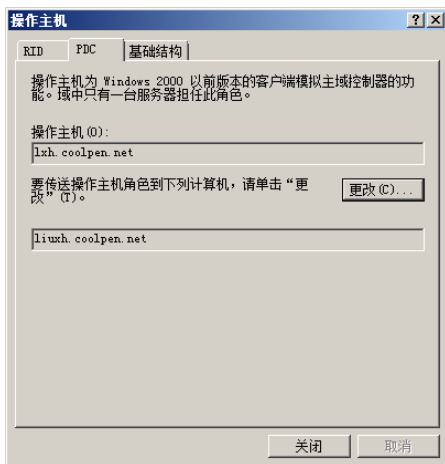


图 3-111 “PDC”选项卡

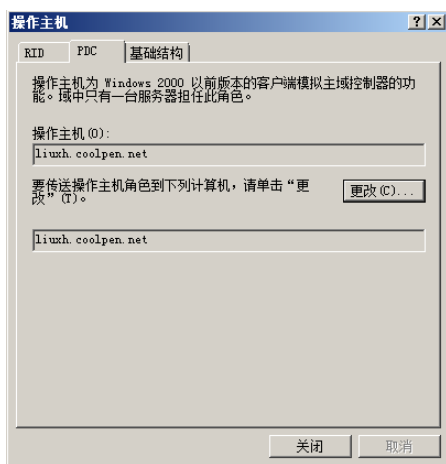


图 3-112 转移 PDC 主机角色

4. 转移结构主机角色

切换到“基础结构”选项卡，单击“更改”按钮将结构主机由原主域控制器转移到辅助域控制器，如图 3-113 所示。单击“关闭”按钮关闭对话框。

5. 转移域命名主机角色

- ① 单击“开始”→“管理工具”→“Active Directory 域和信任关系”选项，显示如图 3-114 所示的“Active Directory 域和信任关系”窗口。
- ② 右击“Active Directory 域和信任关系”选项，在快捷菜单中选择“操作主机”选项，显示如图 3-115 所示的“操作主机”对话框。在“域命名操作主机”文本框中显示的是原主域控制器的计算机名，在“要将域命名主机角色转移到下列计算机”文本框中显示的是辅助域控制器的计算机名。

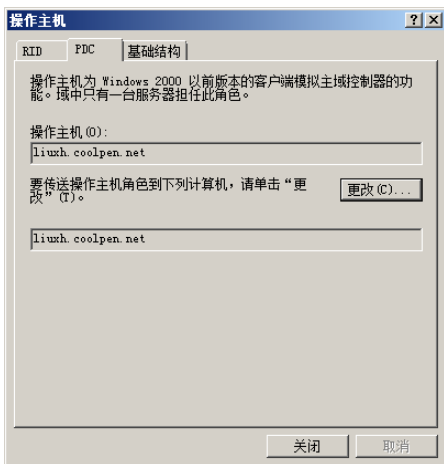


图 3-113 转移结构主机角色

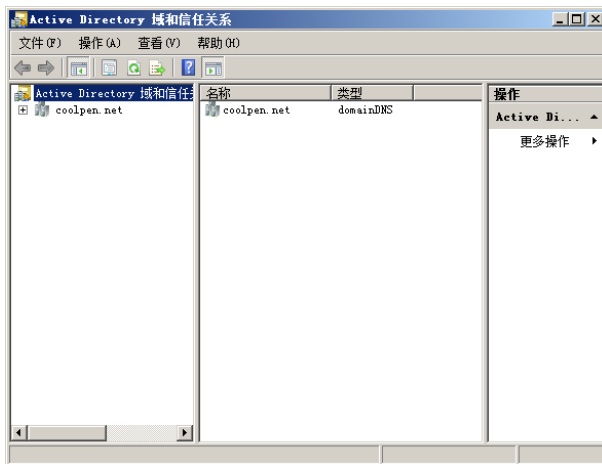


图 3-114 “Active Directory 域和信任关系”窗口

- ③ 单击“更改”按钮，显示如图 3-116 所示的提示框，询问是否要将操作主机角色转移到不同的计算机。

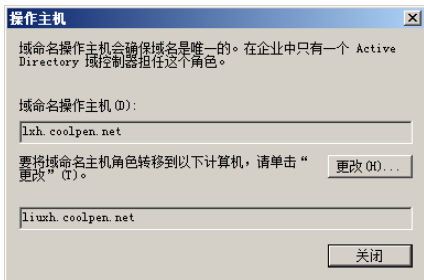


图 3-115 “操作主机”对话框

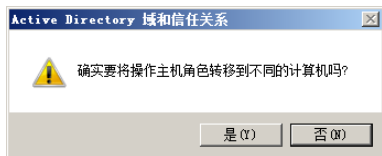


图 3-116 提示框

- ④ 单击“是”按钮，转移操作主机角色并显示如图 3-117 所示的提示框，提示已转移成功。
- ⑤ 单击“确定”按钮，返回到“操作主机”对话框。域命名主机角色转移完成，如图 3-118 所示。单击“关闭”按钮。



图 3-117 提示框



图 3-118 域命名主机角色转移完成

6. 转移架构主机角色

- ① 为转移架构主机角色，打开“命令提示符”窗口，输入如下命令：

```
ntdsutil
```

按回车键，进入 ntdsutil 命令提示符，输入如下命令：

```
roles
```

按回车键，进入 fsmo maintenance 命令提示符，输入如下命令：

```
connections
```

按回车键，进入 server connections 命令提示符，输入如下命令连接辅助域控制器：

```
connect to server liuxh.coolpen.net
```

按回车键，提示如图 3-119 所示的命令成功执行信息，其中 liuxh.coolpen.net 是目标辅助域控制器的计算机名。

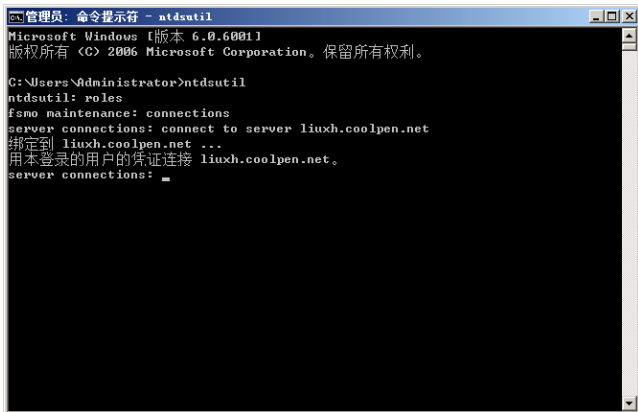


图 3-119 连接辅助域控制器

- ② 在 server connections 提示符下，输入如下命令：

Quit

按回车键，返回 fsmo maintenance 命令提示符。

- ③ 在 fsmo maintenance 命令提示符下，输入如下命令：

Transfer schema master

④ 按回车键，显示如图 3-120 所示的“角色传送确认对话”对话框，提示网络管理员是否需要将架构主机角色传送到目标服务器中。

⑤ 单击“是”按钮，将架构主机角色传送到目标服务器中，如图 3-121 所示，然后执行两次 Quit 命令退出 Ntdsutil 程序。



图 3-120 “角色传送确认对话”对话框

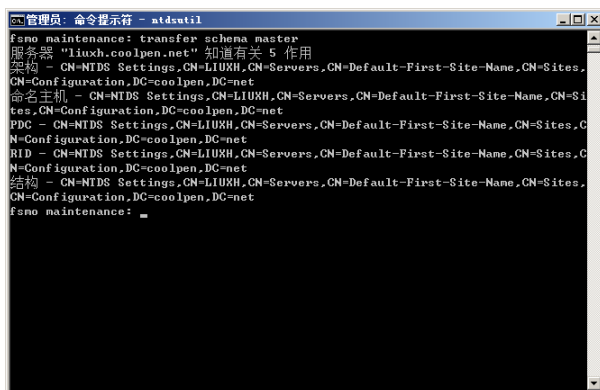


图 3-121 将架构主机角色传送到目标服务器中

7. 查看架构主机角色

使用“Active Directory 架构”管理单元可以查看架构主机角色的位置。不过默认状态下，“Active Directory 架构”并没有在 MMC 管理单元中显示，需要网络管理员注册后才可使用。

① 在辅助域控制器中单击“开始”→“运行”选项，打开如图 3-122 所示的“运行”对话框，在“打开”文本框中输入命令 regsvr32 schmmgmt.dll。

- ② 单击“确定”按钮，显示如图 3-123 所示的“Regsvr32”注册成功提示框。

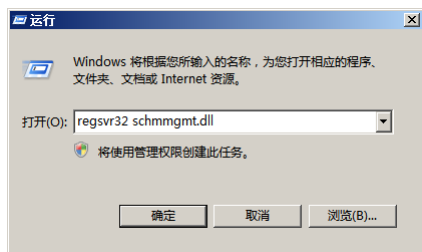


图 3-122 “运行”对话框



图 3-123 “Regsvr32”注册成功提示框

- ③ 单击“确定”按钮完成注册。

④ 单击“开始”→“运行”选项，运行“MMC”命令打开控制台窗口。单击“文件”→“添加或删除管理单元”选项，显示如图 3-124 所示的“添加或删除管理单元”对话框。在“可用的管理单元”下拉列表框中选择“Active Directory 架构”选项，单击“添加”按钮添加到“所选管理单元”列表框中。

⑤ 单击“确定”按钮，关闭“添加或删除管理单元”对话框。返回到控制台窗口，已添加“Active Directory 架构”管理单元，如图 3-125 所示。

- ⑥ 右击“Active Directory 架构”选项，在快捷菜单中选择“操作主机”选项，显示如图 3-126

所示的“更改架构主机”对话框。可以看到，架构主机角色已经由 lxh.coolpen.net 转移到辅助域控制器 liuxh.coolpen.net 中。

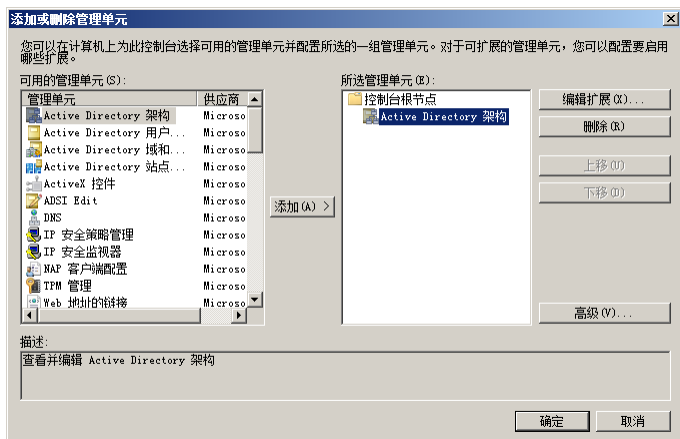


图 3-124 “添加或删除管理单元”对话框

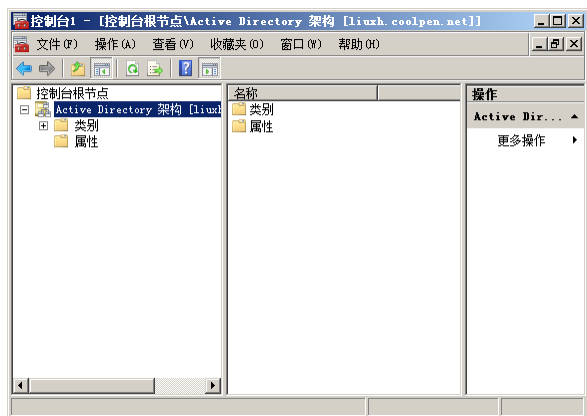


图 3-125 已添加“Active Directory 架构”管理单元

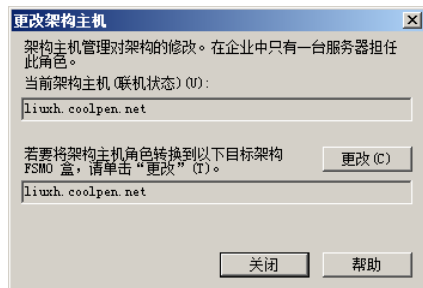


图 3-126 “更改架构主机”对话框

3.4.3 恢复原主域控制器

将主域控制器角色转移到辅助域控制器上以后，需要将其提升为全局编录服务器，并在原来的主域控制器上运行 dcpromo.exe 命令删除原来的域控制器。然后重新安装 Windows Server 2008，并升级为辅助域控制器，最后提升为主域控制器。

1. 升级辅助域控制器为全局编录服务器

这里原主域控制器计算机名称为“lxh”，域名为“coolpen.net”，辅助域控制器的计算机名为“liuxh”。将要把计算机 liuxh 提升为新主域控制器，在原辅助域控制器上执行如下操作。

① 单击“开始”→“管理工具”→“Active Directory 站点和服务”选项，显示如图 3-127 所示的“Active Directory 站点和服务”窗口，依次展开“Sites”→“Default-First-Site-Name”→“Servers”→“liuxh”选项。

② 右击“NTDS Settings”选项，在快捷菜单中选择“属性”选项，显示的如图 3-128 所示的“NTDS Settings 属性”对话框。在“查询策略”下拉列表框中选择“Default Query Policy”选项，并选中“全局编录”复选框。

③ 单击“确定”按钮，显示如图 3-129 所示的警告框，提示是否要使该域控制器成为全局编录。

④ 单击“是”按钮，该域控制器即可成为全局编录服务器。

至此，原来的辅助域控制器即升级为主域控制器，并承担原主域控制器的所有工作。

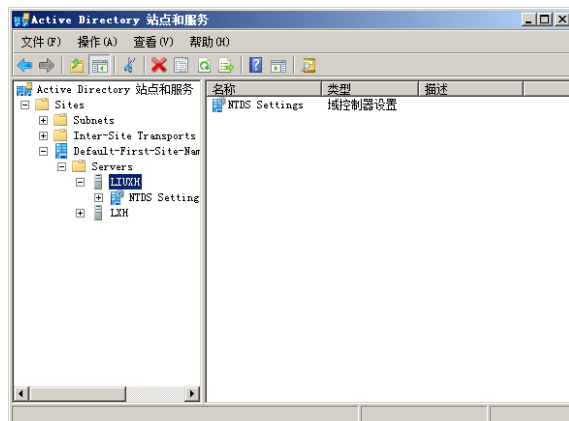


图 3-127 “Active Directory 站点和服务”窗口

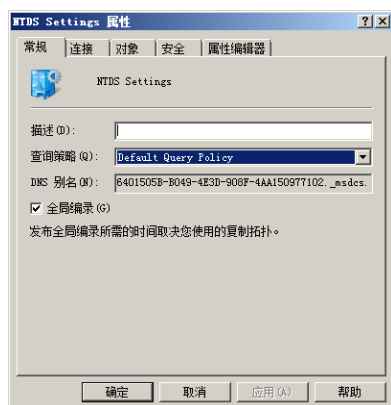


图 3-128 “NTDS Settings”对话框

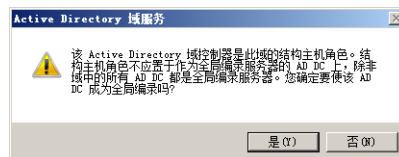


图 3-129 警告框

2. 恢复原主域控制器

在原来的主域控制器（现已经降级为辅助域控制器，计算机名为 lxh）上执行如下操作。

- ① 运行 dcpromo 命令，启动“Active Directory 域服务安装向导”。单击“下一步”按钮，显示如图 3-130 所示的提示框。
- ② 单击“确定”按钮，显示如图 3-131 所示的“删除域”对话框。注意，由于本网络中还存在有其他域控制器，因此不能选中“删除该域，因为此服务器是该域中的最后一个域控制器”复选框。



图 3-130 提示框

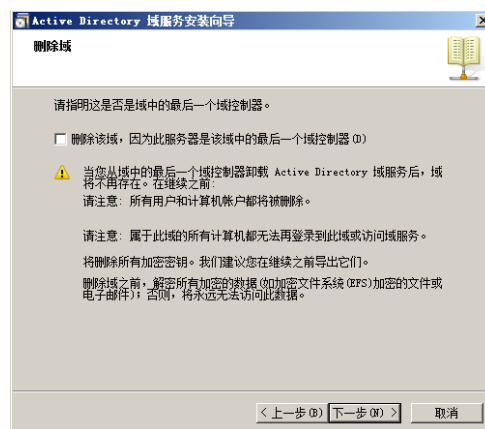


图 3-131 “删除域”对话框

- ③ 单击“下一步”按钮，显示如图 3-132 所示的“Administrator 密码”对话框，在“密码”和“新密码”文本框中为 Administrator 账户设置一个新密码。

④ 单击“下一步”按钮，显示如图 3-133 所示的“摘要”对话框。提示将从该计算机上删除域服务，删除后将成为域的成员。



图 3-132 “Administrator 密码”对话框

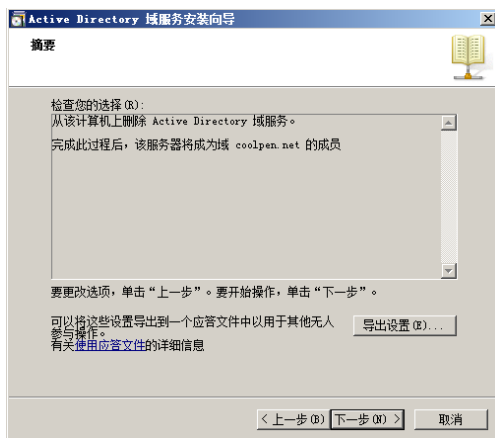


图 3-133 “摘要”对话框

⑤ 单击“下一步”按钮，开始将目录分区中的剩余数据传送到原来的辅助域控制器中并删除域服务，如图 3-134 所示。

提示 如果在运行过程中重启过服务器，或者断开了网络连接，则会提示无法将目录分区的剩余数据传送到其他域控制器。此时可再次在命令提示符中运行命令“ntdsutil”→“roles”→“connections”→“connect to server liuxh.coolpen.net”，连接原来的辅助域控制器。

⑥ 域服务删除完成后，显示如图 3-135 所示的“完成 Active Directory 域服务安装向导”对话框，提示已删除域服务。

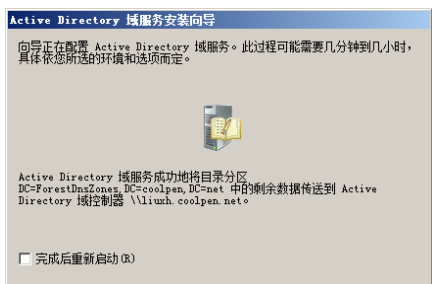


图 3-134 删除域服务

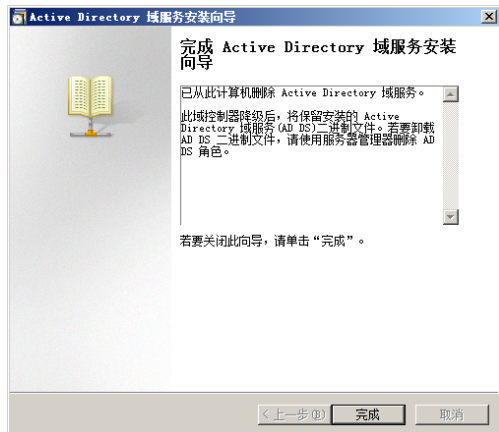


图 3-135 “完成 Active Directory 域服务安装向导”对话框

⑦ 单击“完成”按钮，并根据系统提示重新启动服务器。
重新启动后，将降级为域的成员。此时可从域中脱离，并重新格式化分区、重新安装 Windows Server 2008。然后将计算机升级为辅助域控制器，再升级到主域控制器，完成后从备份中恢复原来数据。至此，Active Directory 域控制器的恢复完成。

3.4.4 占用操作主机角色

如果网络中的主域控制器已经完全损坏，并且不能恢复，为了保证网络的正常运行，此时可以将辅助域控制器“强行”升级为 Active Directory 的主域控制器及全局编录服务器。然后重新安装原来的

主域控制器，升级为辅助域控制器再升级为主域控制器即可。

① 在命令提示符下输入如下命令：

```
ntdsutil
```

按回车键，进入 ntdsutil 命令提示符，输入如下命令：

```
roles
```

按回车键，进入 fsmo maintenance 命令提示符，输入如下命令：

```
connections
```

按回车键，进入 server connections 命令提示符，输入如下命令：

```
connect to server liuxh.coolpen.net
```

按回车键，命令行成功执行，如图 3-136 所示，其中 liuxh.coolpen.net 是辅助域控制器的计算机名。

② 在 server connections 提示符下，输入 Quit 命令，返回 server connections 命令提示符。

③ 占用“架构主机”角色，在 fsmo maintenance 命令提示符下，输入如下命令：

```
Seize schema master
```

按回车键，显示如图 3-137 所示的“角色占用确认对话”对话框，提示网络管理员是否需要占用架构主机角色。



图 3-136 连接辅助域控制器



图 3-137 “角色占用确认对话”对话框

单击“是”按钮，将占用架构主机角色，如图 3-138 所示。

④ 占用 RID 主机角色，在 fsmo maintenance 命令提示符下，输入如下命令：

```
Seize RID master
```

按回车键，显示如图 3-139 所示的“角色占用确认对话”对话框，提示网络管理员是否需要占用 RID Master 主机角色。

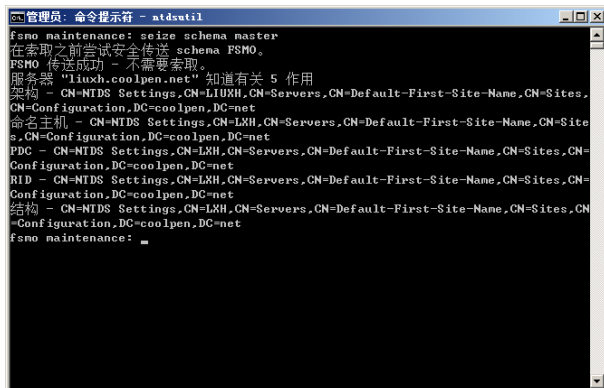


图 3-138 占用架构主机角色



图 3-139 “角色占用确认对话”对话框

单击“是”按钮，占用 RID Master 主机角色，如图 3-140 所示。

⑤ 占用 PDC 模拟器角色，在 fsmo maintenance 命令提示符下，输入如下命令：

```
Seize PDC
```

按回车键，显示如图 3-141 所示的“角色占用确认对话”对话框，提示网络管理员是否需要占用 PDC 主机角色。

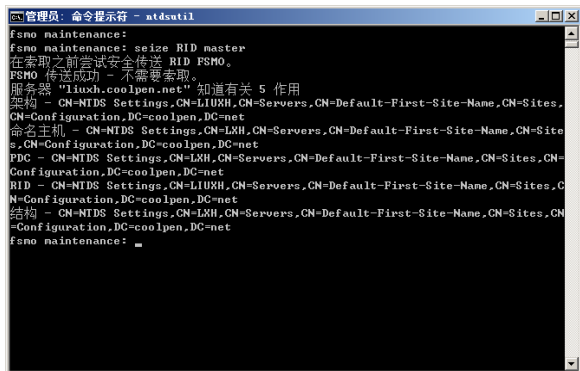


图 3-140 占用 RID 主机角色



图 3-141 “角色占用确认对话”对话框

单击“是”按钮，占用 PDC 主机角色，如图 3-142 所示。

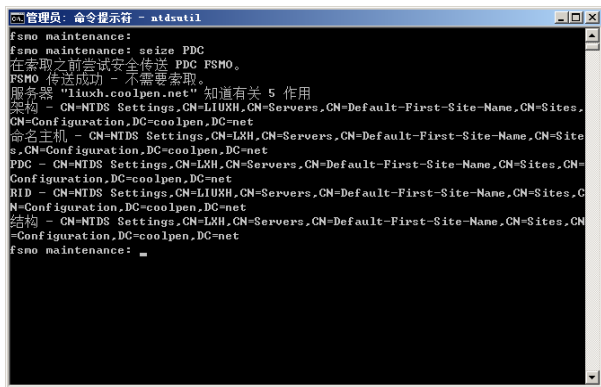


图 3-142 占用 PDC 角色

⑥ 占用结构主机角色，在 fsmo maintenance 命令提示符下，输入如下命令：

```
Seize infrastructure master
```

按回车键，显示如图 3-143 所示的“角色占用确认对话”对话框，提示网络管理员是否需要占用 infrastructure master 主机角色。

单击“是”按钮，占用 infrastructure master 主机角色，如图 3-144 所示。



图 3-143 “角色占用确认对话”对话框

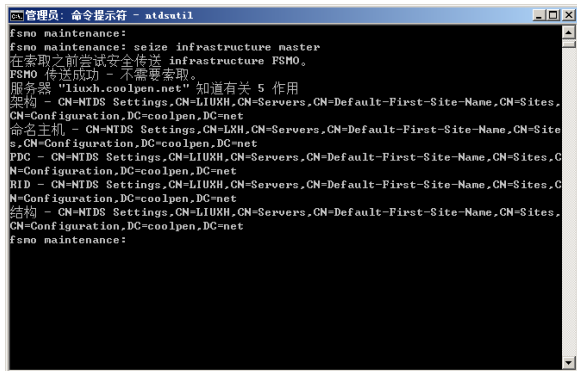


图 3-144 infrastructure master 主机角色

⑦ 占用域命名主机角色，在 fsmo maintenance 命令提示符下，输入如下命令：

```
Seize naming master
```

按回车键，显示如图 3-145 所示的“角色占用确认对话”对话框，提示网络管理员是否需要占用 naming master 主机角色。

单击“是”按钮，占用 naming master 主机角色，如图 3-146 所示。

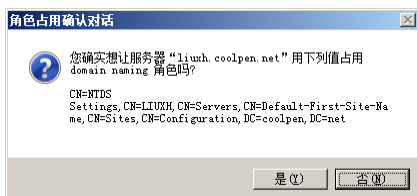


图 3-145 “角色占用确认对话”对话框

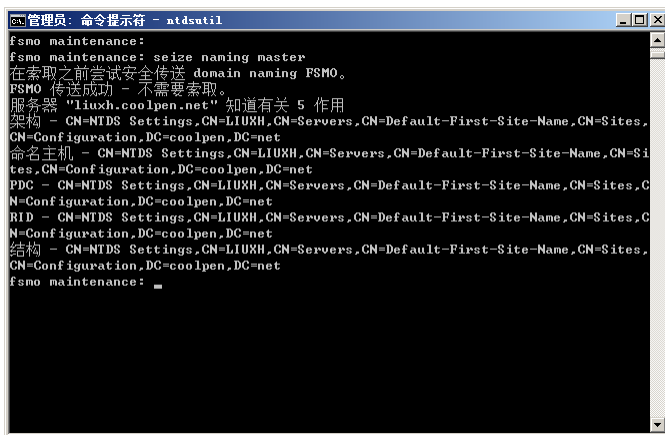


图 3-146 占用 naming master 主机角色

⑧ 输入两次“quit”，退出 Ntdsutil 程序，返回命令提示符窗口。

至此，辅助域控制器已占用了主域控制器角色，然后升级为全局编录服务器即可。具体操作过程可参见前面所述内容，这里不再赘述。

3.5 域信任关系

当网络中存在多个不同的域时，为了使用户可以自由地访问网络中的每台服务器（无论用户是否属于待登录的域），多个域之间需要创建信任关系。信任关系是两个域控制器之间实现资源互访的重要前提，其中信任域负责受信域的登录验证；受信域中定义的用户账户和全局组可以获得信任域的权利和权限，即使该用户账户或组不在信任域的目录中。

3.5.1 信任关系

根据信任关系是否具有传递性，可以分为可传递信任和非可传递信任。传递性确定了信任是否可以扩展到建立信任的两个域之外。可传递信任用于将信任关系扩展到其他域，而非传递信任用于拒绝与其他域之间的信任关系。

1. 可传递信任

每次在林中创建新的域时，在新域及其父域之间会自动创建双向的可传递信任关系。如果子域被添加到新的域中，则信任路径将通过域层次向上流动，从而扩展到新域与其父域之间创建的初始信任路径。

可传递信任关系将以域树形成时的方向沿域树向上流动，最终在域树中的所有域之间创建可传递信任。身份验证请求遵循这些信任路径，因此来自林的任何域中的账户可在林中的任何其他域中进行验证。通过单个登录进程，拥有相应权限的账户可访问林中任何域中的资源。

如图 3-147 所示为域树 A.B.C.com 中的所有域和域树 1.com 中的所有域在默认情况下具有可传递信任关系。因此当为资源指派适当的权限后，域树 A.B.C.com 中的用户可以访问域树 1.com 中的资源，域树 1.com 中的用户可以访问域树 A.B.C.com 中的资源。

除了 Windows Server 2008 林中建立的默认可传递信任之外，还可以使用“新建信任向导”手动创

建可传递信任，包括如下类型。

(1) 快捷信任：在相同域树或林中的域之间的可传递信任，用于缩短大型复杂的域树或林中的信任路径。

(2) 林信任：在林根域和第2个林根域之间的可传递信任。

(3) 领域信任：在 Active Directory 域 Kerberos V5 领域之间的可传递信任。

有时信任关系并不是由于加入域目录树或用户创建产生的，而是由彼此之间的传递性而得到的，这种信任关系也被称为“隐含的信任关系”。如图 3-148 所示是由于信任关系的双向传递性而得出的隐含信任关系，其中域 A 与域 B 及域 A 与域 C 相互信任，由此也就得出了域 C 和域 B 之间的信任关系。

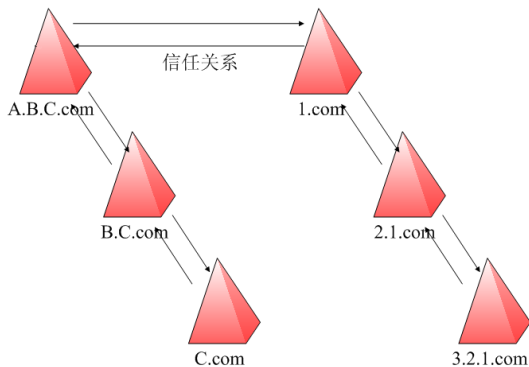


图 3-147 可传递信任关系

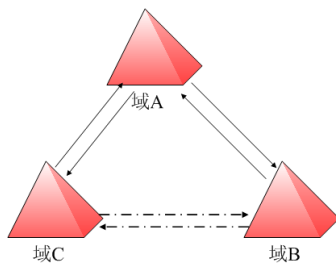


图 3-148 隐含信任关系

2. 非传递信任

非传递信任受信任关系中的两个域的约束，并不流向林中的任何其他域。它可以是双向信任或单向信任，默认为单向信任关系，但用户也可通过建立两个单向信任来建立一个双向关系。总的来说，不可传递域信任是以下各项之间唯一的信任关系形式。

(1) Windows Server 2003/2008 域和 Windows NT 域。

(2) 一个林中的 Windows Server 域和另一个林中的某个域（当没有被林信任连接时）。

用户可以使用 Active Directory 域和信任关系中的“新建信任向导”手动创建下列非传递信任。

(1) 外部信任：在 Windows Server 域和 Windows NT 域或者另一个林中的 Windows Server 域或者 Windows 2000 域之间创建的非传递信任。

(2) 领域信任：在 Active Directory 域和 Kerberos V5 领域之间的非传递信任。

当把 Windows NT 域升级到 Windows Server 2003/2008 域时，所有现有的 Windows NT 信任都保持不变，在 Windows Server 2003/2008 域和 Windows NT 域之间的所有信任关系都是不可传递的。

3.5.2 设置域信任关系

当网络中有多个不同的域时，需要在待设置为信任的每台域控制器上都创建信任，使其分别信任对方域控制器。这里以两个域建立信任关系为例，一个域是 coolpen.net；另一个域是 hsnc.cn。不过在建立信任之前，必须首先将各个域控制器的 DNS 服务器地址设置为对方域控制器的 IP 地址。首先在域控制器 coolpen.net 上创建信任关系。

① 单击“开始”→“管理工具”→“Active Directory 域和信任关系”选项，打开“Active Directory 域和信任关系”窗口。右击域名 coolpen.net，选择快捷菜单中的“属性”选项，打开如图 3-149 所示的“coolpen.net 属性”对话框。

② 打开如图 3-150 所示的“信任”选项卡，在信任列表中创建信任。

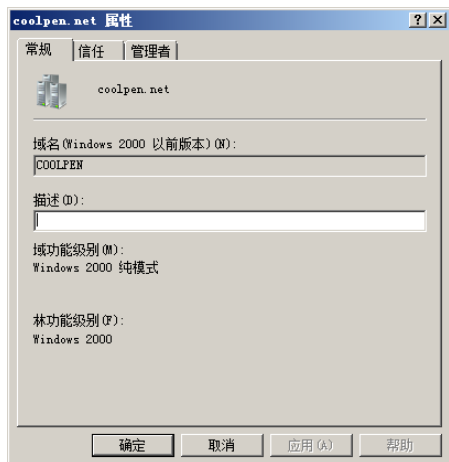


图 3-149 “coolpen.net 属性”对话框

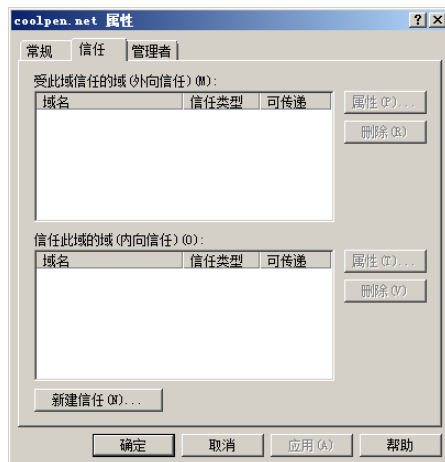


图 3-150 “信任”选项卡

提示

如果该域包含有子域，则会自动和子域建立信任，并显示在信任列表中。

③ 单击“新建信任”按钮，打开如图 3-151 所示的新建信任向导。

④ 单击“下一步”按钮，显示如图 3-152 所示的“信任名称”对话框，在“名称”文本框中输入需要与之建立信任关系域的 NetBIOS 名称。

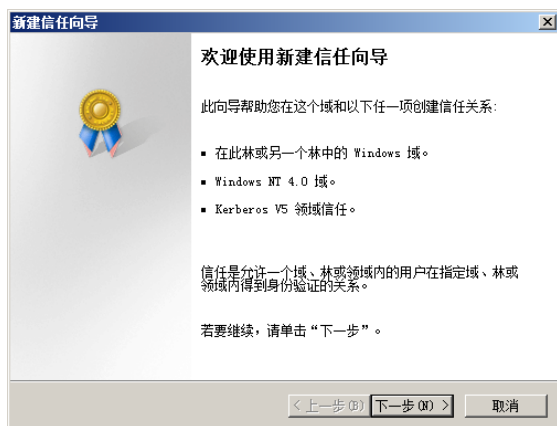


图 3-151 新建信任向导

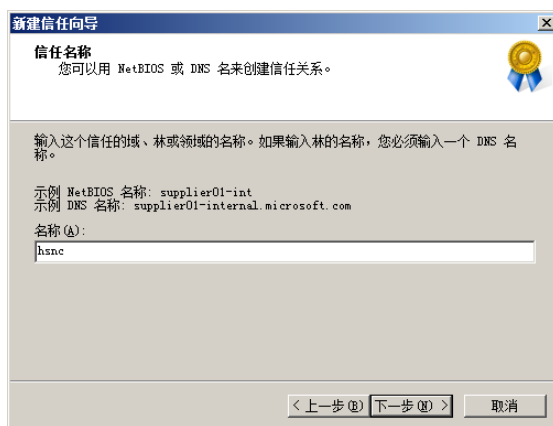


图 3-152 “信任名称”对话框

提示

此处应输入 NetBIOS 名称。如果要输入 DNS 名称，则本地服务器的 DNS 服务器必须设置为对方域控制器的 IP 地址；否则无法解析。

⑤ 单击“下一步”按钮，显示如图 3-153 所示的“信任方向”对话框。有 3 个选项可供选择，其中选择“双向”传递信任，则该域中的用户可以在指定域、领域或域林中得到身份验证；反之亦然。单向传递又可以划分为“单向：内传”和“单向：外传”，分别表示该域中的用户可以在指定域、领域或域林中得到身份验证和指定域、领域或域林的用户可以在该域中得到身份验证，这两种情况均是单向信任；反之则不成立。这里选择“双向”单选按钮。

⑥ 单击“下一步”按钮，显示如图 3-154 所示的“信任方”对话框。如果仅与这一个域建立信任关系，则选择“只是这个域”单选按钮；如果也与指定域建立信任关系，则选择“此域和指的域”单选按钮。

⑦ 单击“下一步”按钮，显示如图 3-155 所示的“传出信任身份验证级别”对话框，为建立信任的域 hsn.cn 中的用户选择身份验证的范围。选择“全域性身份验证”单选按钮，可以自动对指定

域的用户使用本地域的所有资源进行验证。如果两个域属于同样的组织时，可选择该单选按钮。选择“选择性身份验证”单选按钮，将不会自动对指定域的用户使用本地域的所有资源进行身份验证，需向指定域用户授予访问权限。如果域之间属于不同组织时，建议选择该单选按钮。

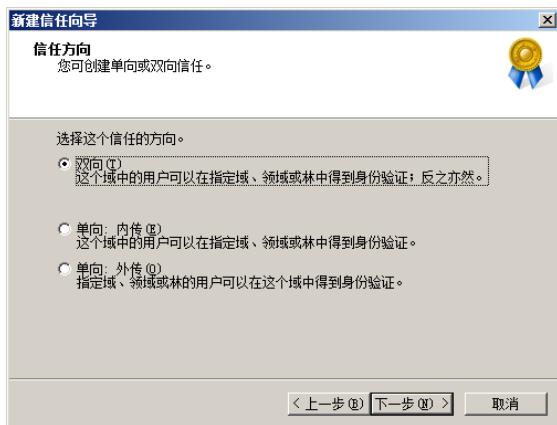


图 3-153 “信任方向”对话框

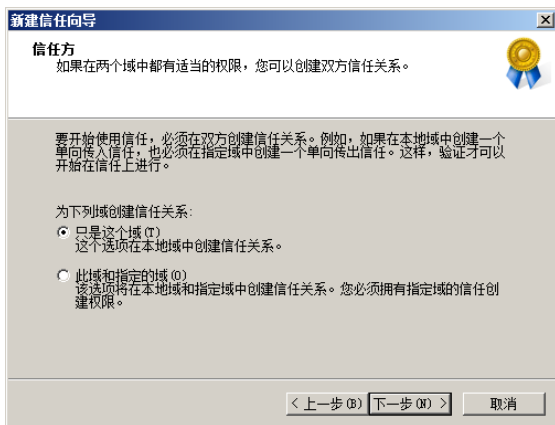


图 3-154 “信任方”对话框

⑧ 单击“下一步”按钮，显示如图 3-156 所示的“信任密码”对话框，设置此信任的密码。

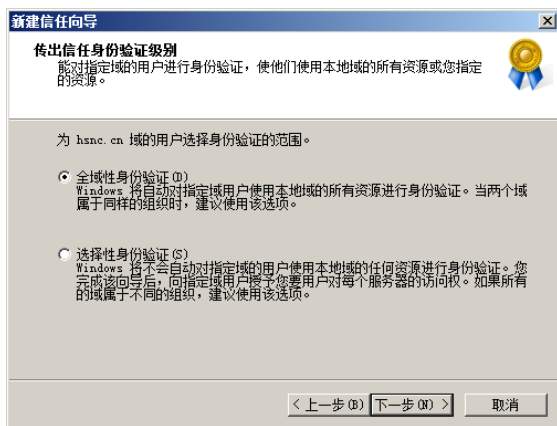


图 3-155 “传出信任身份验证级别”对话框

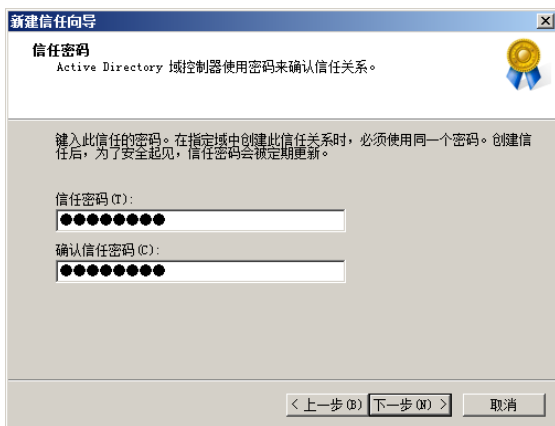


图 3-156 “信任密码”对话框

⑨ 单击“下一步”按钮，显示如图 3-157 所示的“选择信任完毕”对话框。其中列出前面所做的配置，如需更改，则单击“上一步”按钮返回。

⑩ 单击“下一步”按钮，显示如图 3-158 所示的“信任创建完毕”对话框，提示信任关系创建成功。

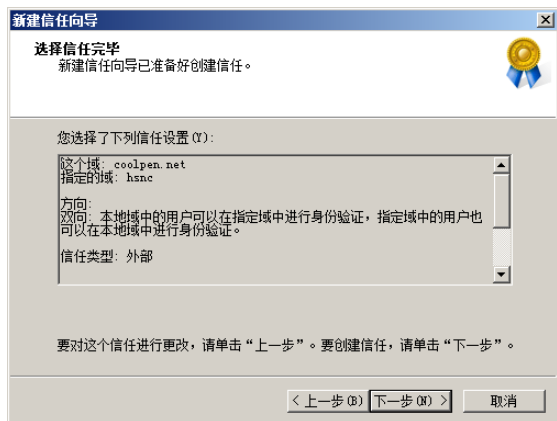


图 3-157 “选择信任完毕”对话框

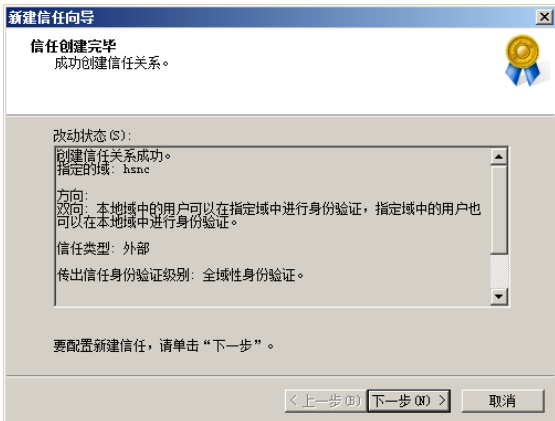


图 3-158 “信任创建完毕”对话框

⑪ 单击“下一步”按钮，显示如图 3-159 所示的“确认传出信任”对话框。选择“否，不要确认传出信任”单选按钮，在另一台域控制器上创建了信任后确认传出信任。

⑫ 单击“下一步”按钮，显示如图 3-160 所示的“确认传入信任”对话框，选择“否，不确认传入信任”单选按钮。



图 3-159 “确认传出信任”对话框



图 3-160 “确认传入信任”对话框

⑬ 单击“下一步”按钮，显示如图 3-161 所示的“正在完成新建信任向导”对话框，提示创建信任关系成功。

⑭ 单击“完成”按钮，域控制器 coolpen.net 上的信任关系创建成功，如图 3-162 所示。

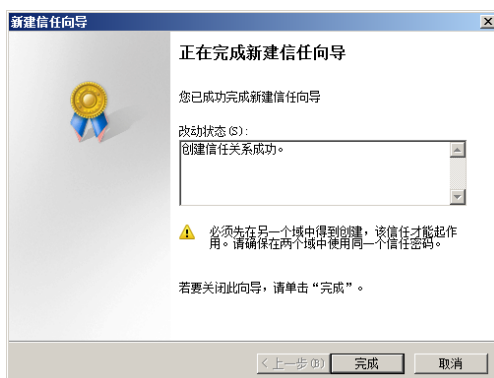


图 3-161 “正在完成新建信任向导”对话框

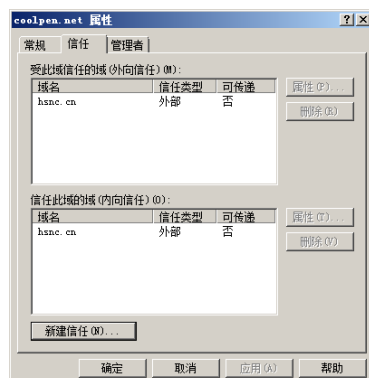


图 3-162 信任关系创建成功

在另一台域控制器 hsnc.cn 上按照同样步骤创建信任关系，不同的是当显示“确认传出信任”对话框时，选择“是，确认传出信任”单选按钮，如图 3-163 所示。

单击“下一步”按钮，显示如图 3-164 所示的“确认传入信任”对话框。选择“是，确认传入信任”单选按钮，并输入 coolpen.net 域中有管理权限的账户名和密码。

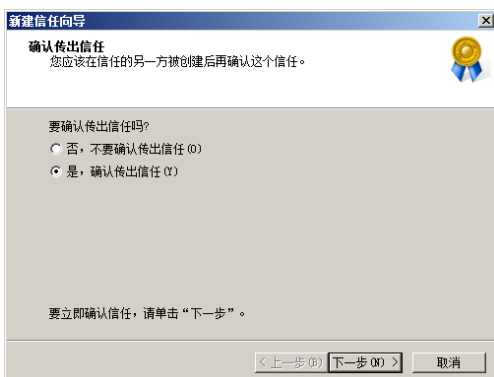


图 3-163 选择“是，确认传出信任”单选按钮

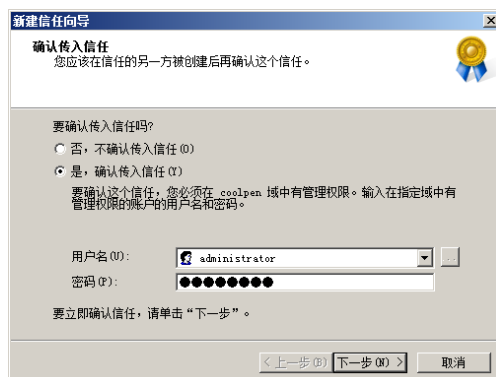


图 3-164 “确认传入信任”对话框

两台域控制器的信任关系创建完成以后,客户端计算机只需加入任何一个域,就可以在如图 3-165 所示的“登录 Windows”对话框中登录时选择登录到另一个域并访问资源,而不需重新加入域。



图 3-165 “登录 Windows”对话框

3.6 用户、组与组织单元

活动目录的主要作用就是管理用户账户,为用户账户分配不同的权限以访问不同的资源。为了便于管理,可以将多个用户添加到组中。为组设置的权限同样适用于组中的所有用户,从而实现对用户的集中管理。而利用组织单元,可以为所有用户和组配置组策略。

3.6.1 用户管理

为了更好地管理网络中的用户,并且使用户更好地使用网络中的资源,应为企业中的每个用户创建一个账号并分配不同的登录权限。

1. 创建用户账户

① 单击“开始”→“管理工具”→“Active Directory 用户和计算机”选项,打开“Active Directory 用户和计算机”窗口。

② 展开左侧树形列表,右击“Users”选项。选择快捷菜单中的“新建”→“用户”选项,显示如图 3-166 所示的“新建对象 - 用户”对话框。输入用户的姓名,并在“用户登录名”文本框中设置用户登录名。为便于记忆,通常使用姓名的拼音简写。如果网络中有多个域,还需要在下拉列表框中选择用户所在的域。

③ 单击“下一步”按钮,在“密码”和“确认密码”文本框中为用户账户设置密码,如图 3-167 所示。

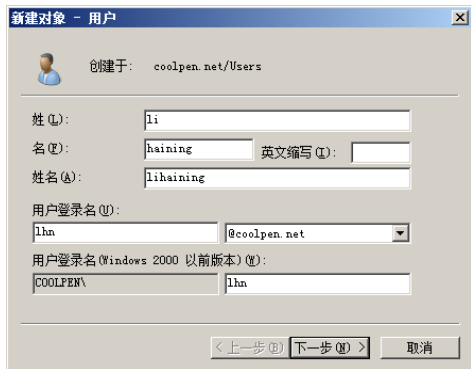


图 3-166 “新建对象 - 用户”对话框

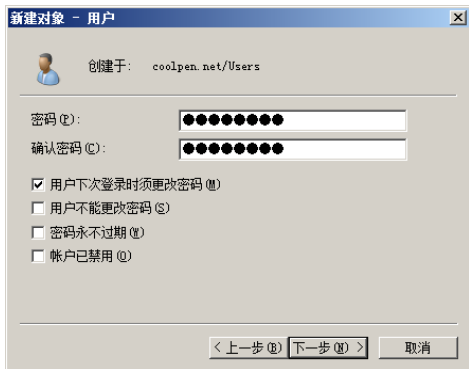


图 3-167 设置密码

并根据需要选择如下选项。

- 用户下次登录时须更改密码: 第 1 次使用该用户账户登录时必须更改密码。
- 用户不能更改密码: 用户能使用该账户登录,但不能自行更改密码。

- 密码永不过期：永远不会提示用户须更改密码。
- 账户已禁用：账户创建后禁止使用。

提示



如果选中“用户下次登录时须更改密码”复选框，则“用户不能更改密码”和“密码永不过期”复选框将不能被选中。

- 单击“下一步”按钮，显示如图 3-168 所示的对话框，其中显示用户设置的摘要信息。

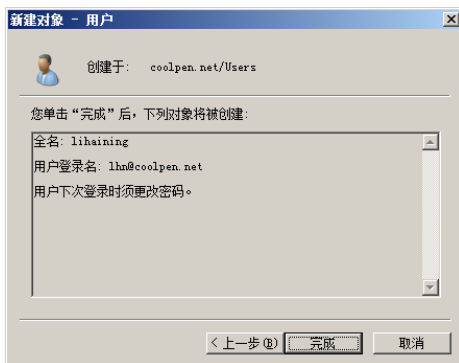


图 3-168 摘要信息

- 单击“完成”按钮，添加完成用户账户，按照同样操作可以继续添加多个用户账户。

2. 设置用户属性

用户账户新建完成之后，只具有最基本的登录权限。还要根据需要配置用户属性，如设置拨入及远程控制权限等。

(1) “常规”选项卡

在“Active Directory 用户和计算机”窗口中，右击用户账户。并选择快捷菜单中的“属性”选项，显示如图 3-169 所示的用户属性对话框。默认为“常规”选项卡，在其中设置用户的常用信息，如账户描述、姓名、电话号码、电子邮件地址和网页等。

(2) “账户”选项卡

打开“账户”选项卡，如图 3-170 所示。在其中设置账户的登录信息，如登录名、登录域、登录时间及限制登录的工作站等。

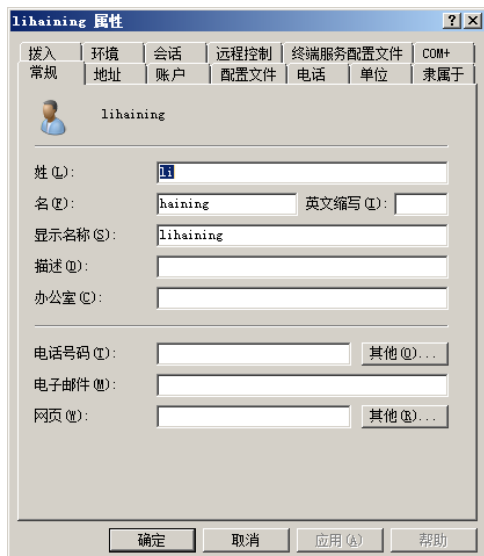


图 3-169 用户属性对话框

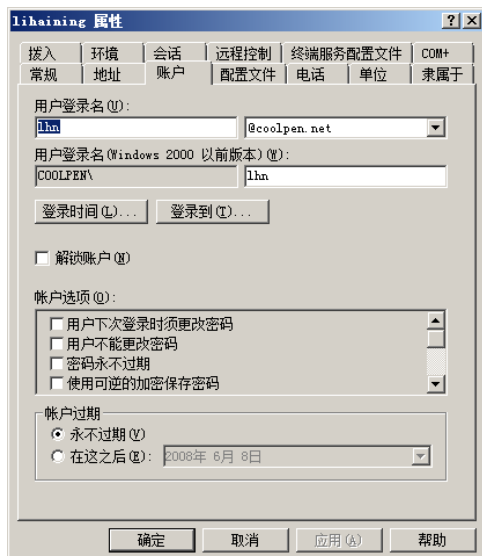


图 3-170 “账户”选项卡

单击“登录时间”按钮，显示“登录时间”对话框。在其中设置该账户的登录时间，默认允许在任何时间内登录域。如果要限制用户在某个特定时间登录，例如，只允许用户在每周一~周五的上午 8 点~下午 17 点登录，则先选中所有区域。单击“拒绝登录”单选按钮使其变为白色，然后选中周一~周五的上午 8 点~下午 17 点区域。单击“允许登录”按钮使其变为蓝色即可，如图 3-171 所示，单击“确定”按钮保存。

在“账户”选项卡中单击“登录到”按钮，显示如图 3-172 所示的“登录工作站”对话框。默认选择“所有计算机”单选按钮，即允许使用该账户登录所有工作站。如果要限制用户账户只能登录特定的计算机，则选择“下列计算机”单选按钮，并在“计算机名称”文本框中输入允许登录的计算机名。单击“添加”按钮添加到列表框中，单击“确定”按钮保存设置。

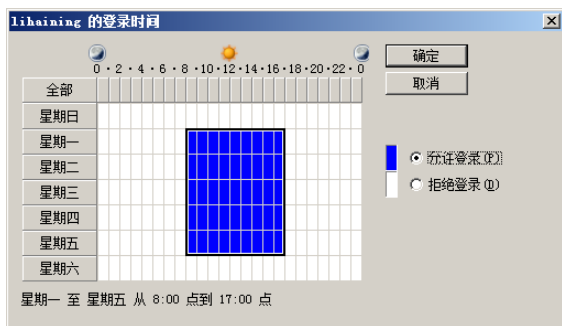


图 3-171 设置登录时间

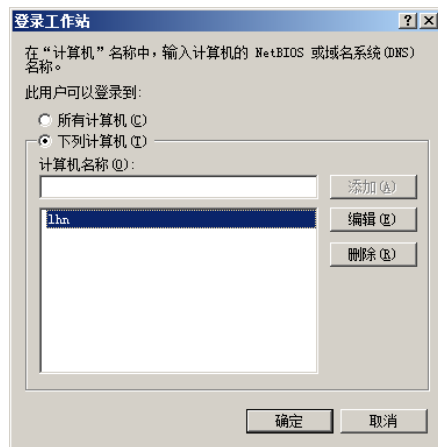


图 3-172 “登录工作站”对话框

(3) “拨入”选项卡

打开如图 3-173 所示的“拨入”选项卡，可以设置用户通过 VPN 等方式拨入到域时所应用的选项，在“网络访问权限”选项组中可以选择是否允许用户拨入。

单击“分配静态 IP 地址”按钮，显示如图 3-174 所示的“静态 IP 地址”对话框，在其中设置当用户使用该账户远程拨入到域后所分配的静态 IP 地址。

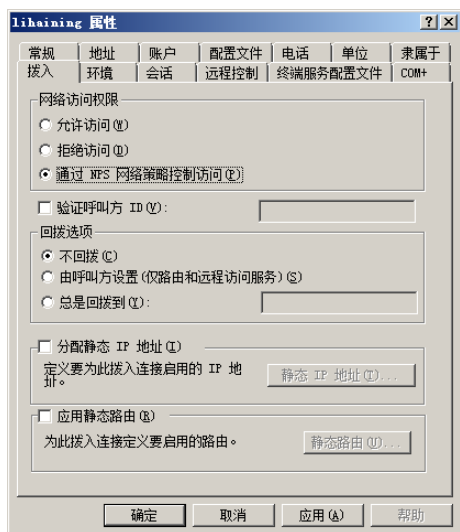


图 3-173 “拨入”选项卡

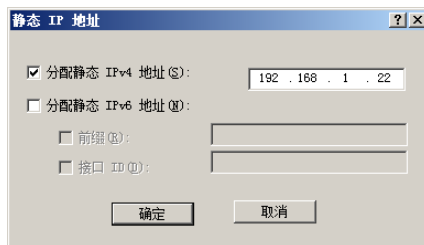


图 3-174 “静态 IP 地址”对话框

在“账户”选项卡中单击“应用静态路由”按钮，显示如图 3-175 所示的“静态路由”对话框，单击“添加路由”按钮来设置使用该账户登录后为该拨入连接启用的静态路由。

3. 添加到组

① 在“Active Directory 用户和计算机”窗口中右击待添加到组的用户账户，选择快捷菜单中的“添加到组”选项。显示如图 3-176 所示的“选择组”对话框，在“输入对象名称来选择”文本框中输入待加入的用户组名称。

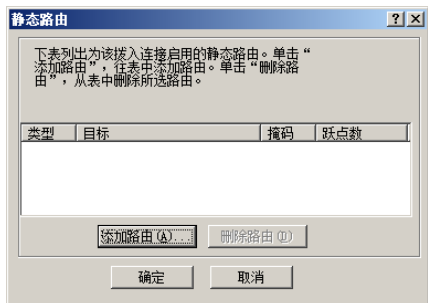


图 3-175 “静态路由”对话框

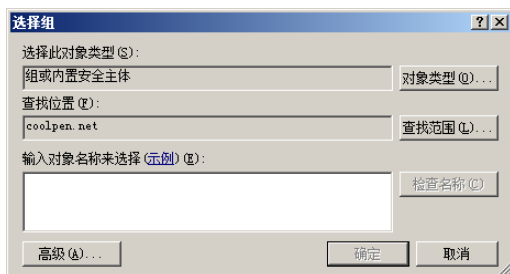


图 3-176 “选择组”对话框

② 如果不知道用户组的确切名称，则单击“高级”按钮。单击“立即查找”按钮，列出域中的所有用户组（如图 3-177 所示），选择待加入的组即可。

提示

如果要同时添加到多个组，可借助 Ctrl 键和 Shift 键来选待加入的组。

③ 单击“确定”按钮，显示如图 3-178 所示的提示框。提示已成功添加该用户账户到所选组中，单击“确定”按钮关闭。

4. 更改密码

① 在“Active Directory 用户和计算机”窗口中右击待更改密码的用户账户，选择快捷菜单中的“更改密码”选项。显示如图 3-179 所示的“重置密码”对话框，在“新密码”和“确认密码”文本框中输入新密码。

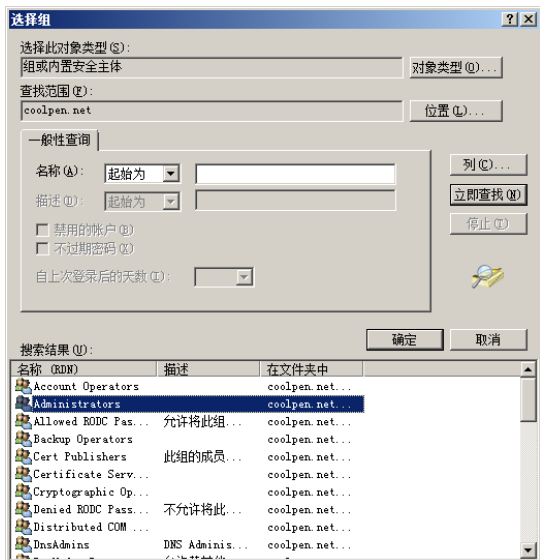


图 3-177 域中的所有用户组

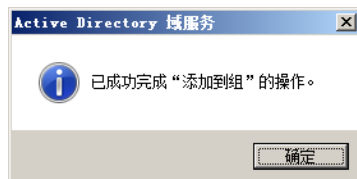


图 3-178 提示框

提示

如果当前账户已被锁定，也可以在该对话框中选“解锁用户的账户”复选框来解除账户的锁定。

- ② 单击“确定”按钮，显示如图 3-180 所示的提示框。提示密码已更改成功，单击“确定”按钮。

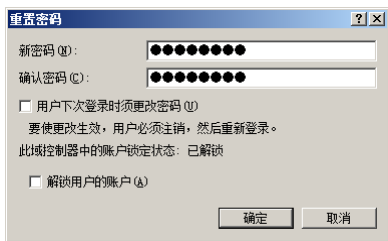


图 3-179 “重置密码”对话框



图 3-180 提示框

5. 重命名账户

右击待重命名的用户账户，选择快捷菜单中的“重命名”选项。该账户名变为可改写状态，如图 3-181 所示。输入一个新的名称，然后按回车键，用户名即可更改成功。

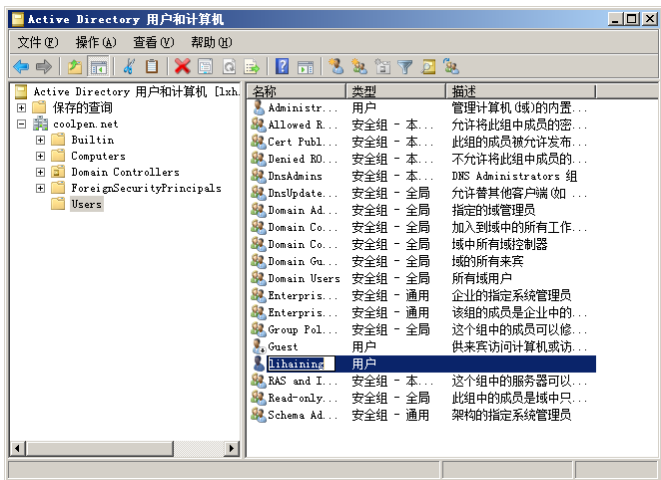


图 3-181 重命名账户

6. 启用、禁用和删除账户

如果有些账户暂时不使用，可以将其禁用，当需要使用时再启用；如果有些账户永远不使用，则可直接将其删除。

在“Active Directory 用户和计算机”窗口中右击待禁用的用户账户，选择快捷菜单中的“禁用账户”选项。显示如图 3-182 所示的提示框，提示账户已被禁用，单击“确定”按钮即可。

如果要重新启用该账户，右击并选择快捷菜单中的“启用账户”选项。显示如图 3-183 所示的提示框，提示该账户已被启用。

如果要删除某个账户，则右击账户名。选择快捷菜单中的“删除”选项，显示如图 3-184 所示的警告框。提示是否要删除该账户，单击“是”按钮即可删除。



图 3-182 提示框



图 3-183 提示框

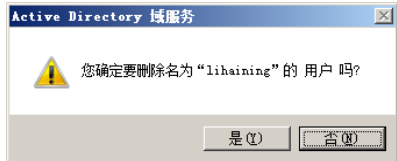


图 3-184 警告框

3.6.2 用户组管理

用户组是管理用户时很常用的功能，可以将多个用户添加到一个组中，通过为该组设置权限就可以起到同时为其中所有用户设置权限的目的。

1. 系统默认组

Active Directory 安装完成之后会自动创建一些具有特殊权限的用户组,存储在 Builtin 容器和 Users 容器中,主要包括如下组。

(1) **Administrators**: 管理员组,该组的成员对域控制器具有完全的控制权限,可以对域控制器执行任何管理任务。

(2) **Domain Admins**: 域管理员组,可以管理整个域,既包括域控制器,也包括所有成员服务器及所有成员工作站。

(3) **Enterprise Admins**: 企业管理员组,存储整个森林的管理员用户账户,即可以管理整个森林,及整个森林中任何一个域。

(4) **Domain Users**: 域用户账户组,存储整个域的用户账户,当新建一个账户时就会自动成为 Domain Users 的成员。

(5) **Everyone**: 这是一个特殊的组,由系统自动生成,但不显示在活动目录中。其中包含所有当前正在访问与控制器的用户,以及 Guest 账户。

(6) **Authenticated Users**: 该组包括 Everyone 用户组中除 Guest 用户账户之外的所有用户。

2. 添加用户组

(1) 打开“Active Directory 用户和计算机”窗口,在左侧树形列表中右击“Users”选项。选择快捷菜单中的“新建”→“组”选项,显示如图 3-185 所示的“新建对象 - 组”对话框。在“组名”文本框中输入新组的名称。在“组作用域”选项区域中选择组的作用域。

- 本地域: 可以添加其他域的账户,但是只能访问此类组所在域的资源。
- 全局: 只能添加该类组所在域的用户账户,不能添加其他域的账户,但是可以访问其他域的资源对象。
- 通用: 可以添加任何域的用户账户,可以访问任何域的资源对象。

在“组类型”选项组中选择组的类型。

- 安全组: 用于与对象权限分配有关的场合。
- 通信组: 用于与安全无关的场合。



图 3-185 “新建对象 - 组”对话框

(2) 单击“确定”按钮,创建完成一个用户组。

3. 设置组的属性

用户组的主要作用是存储用户,以集中管理,因此组建完成后应添加用户。另外,和用户账户一样,也可以对用户组执行重命名、删除及添加到其他组等操作,而且操作方法相同。

(1) “常规”选项卡

在“Active Directory 用户和计算机”窗口中右击待设置的用户组,选择快捷菜单中的“属性”选

项,显示如图 3-186 所示的组属性对话框。默认为“常规”选项卡,可以在其中设置适用于 Windows 2000 以前版本的组名称、组的描述、电子邮件,并且更改组作用域和类型等。

(2) “成员”选项卡

打开如图 3-187 所示的“成员”选项卡,可以在其他组中添加用户账户。

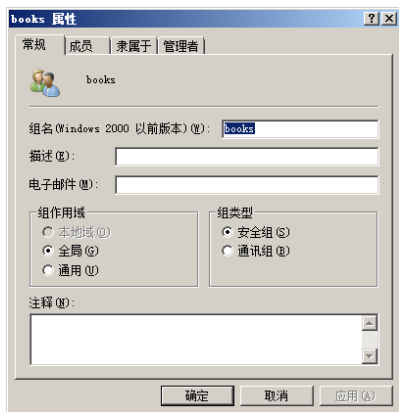


图 3-186 组属性对话框

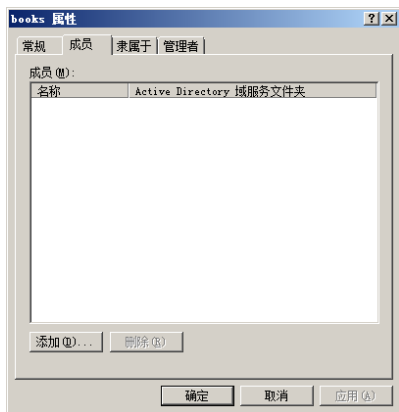


图 3-187 “成员”选项卡

单击“添加”按钮,显示如图 3-188 所示的“选择用户、联系人、计算机或组”对话框,在其中可以查找待添加的用户。

如果当前域中包含多个域,并且每个域中都包括大量用户,则指定查找用户的位置。单击“查找范围”按钮,显示如图 3-189 所示的“位置”对话框。选择待查找的域或容器,单击“确定”按钮返回。

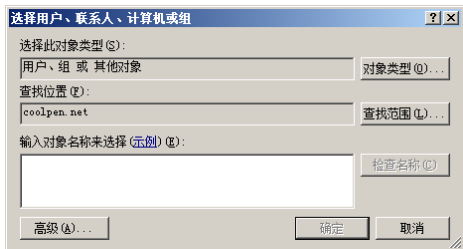


图 3-188 “选择用户、联系人、计算机或组”对话框



图 3-189 “位置”对话框

单击“高级”按钮,单击“立即查找”按钮,列出域中的所有用户账户。可借助 Ctrl 或 Shift 键选择待添加到组中的多个用户账户,如图 3-190 所示。



图 3-190 选择多个用户账户

单击“确定”按钮，所选用户账户被添加到该组中，如图 3-191 所示。

单击“应用”按钮保存设置。

(3) “隶属于”选项卡

打开如图 3-192 所示的“隶属于”选项卡，单击“添加”按钮将该用户组添加到其他组中。

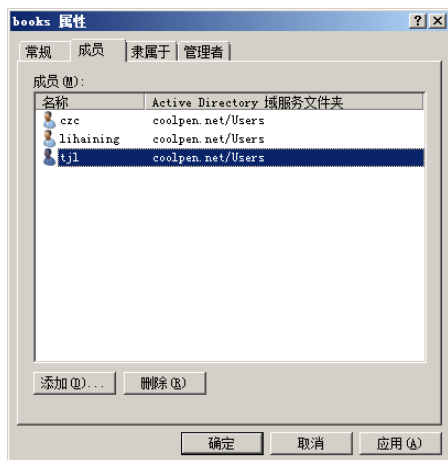


图 3-191 添加的用户

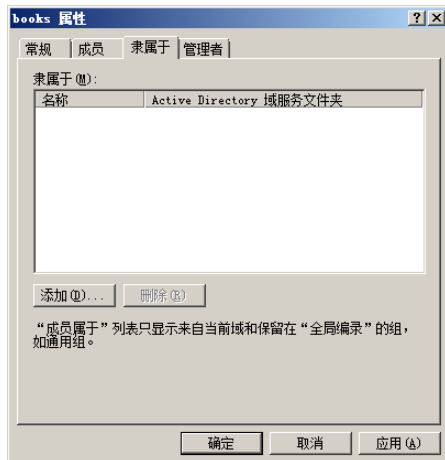


图 3-192 “隶属于”选项卡

3.6.3 组织单位管理

组织单位即组织单元（OU）是一个容器对象，可以把域中的对象组织成逻辑组，从而简化管理工作。OU 可以包含各种对象，如用户、组、计算机及打印机等，甚至可以包括其他 OU。对于企业来讲，可以按部门把所有的用户和设备组成一个 OU，也可以按地理位置组成 OU，还可以按功能和权限分成多个 OU。

① 在“Active Directory 用户和计算机”窗口中右击待新建 OU 的域控制器名称，选择快捷菜单中的“新建”→“组织单位”选项，显示如图 3-193 所示的“新建对象 - 组织单位”对话框。

提示 选中“防止容器被意外删除”复选框可防止意外删除该容器。当执行删除 OU 操作时就会显示如图 3-194 所示的提示框，提示没有足够的权限。

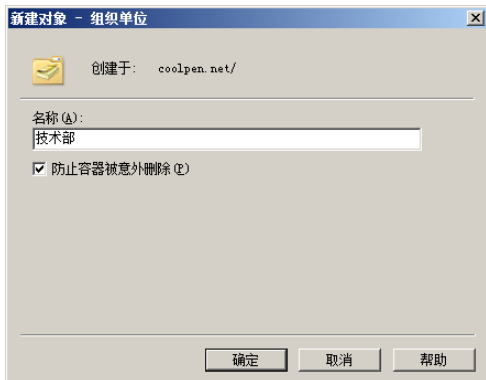


图 3-193 “新建对象 - 组织单位”对话框



图 3-194 提示框

② 在“名称”文本框中键入合适的 OU 名称，单击“确定”按钮。创建完成一个新的组织单位，如图 3-195 所示。

③ 创建完成组织单位后可以在其中添加对象，拖动待添加的对象到组织单位名称上。显示如图 3-196 所示的提示框，单击“是”按钮即可添加到组织单位中。

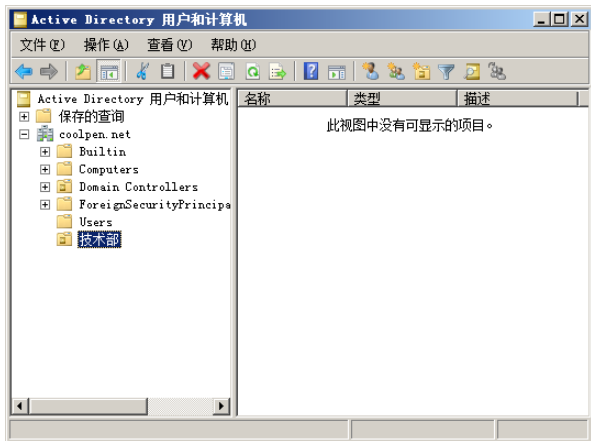


图 3-195 创建完成一个新的组织单位

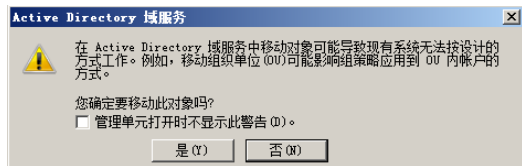


图 3-196 提示框

3.7 组策略及其应用

组策略（Group Policy，GP）是介于控制面板和注册表之间的一种修改系统选项及设置程序的工具，是系统管理员为计算机和用户定义用来控制应用程序、系统设置和管理模板的一种机制。通过组策略可以管理批量用户和计算机，从而提高工作效率。

3.7.1 概述

在 Windows 2008 Server Active Directory 环境中可以管理整个 Active Directory 用户，组策略设置系统管理员需要管理的用户桌面环境的多种组件。例如，用户可运行的程序、用户的桌面环境、“开始”菜单选项及任务栏选项等。它允许系统管理员为特定用户组创建特殊的桌面配置，并且使用的特定的管理单元。指定的组策略设置包含在组策略对象中，而组策略对象又与选定的 Active Directory 对象（即站点、域或组织单位）相关联。

1. 组策略的功能

基于活动目录的组策略不仅应用于用户和客户端，还应用于成员服务器、域控制器，以及管理范围内的任何 Windows 2000 以上操作系统的计算机。默认情况下，应用于根域的组策略会影响域中的所有计算机和组织单位下的用户。Active Directory 用户和计算机管理单元还提供内置的域控制器组织单位。如果将在其中保存域控制器账户，则可以使用组策略对象“默认域控制器策略”将域控制器与其他计算机分开管理。

组策略包括影响用户的“用户配置”和影响计算机的“计算机配置”策略设置，企业通过组策略能够设置集中化和分散化策略、确保用户处于所需的工作环境中，并控制用户和计算机的环境等。

2. 组策略的组件

组策略组件包括组策略对象、组策略模板、组策略容器、客户端扩展、组策略编辑器、计算机策略和用户策略、组策略，以及本地策略组件。

（1）组策略对象组件

在 AD 中包括站点、域和组织单位（OU）在内的容器对象都可以连接到一个 GPO（Group Policy Object，组策略对象）中，通过连接，可以将 GPO 设置应用于所指定容器中的用户和计算机。GPO 由组策略容器（Group Policy Container，GPC）和组策略模板（Group Policy Template，GPT）组成。

（2）组策略模板组件

组策略模板组件实现了一系列的指令集，例如更新注册表的策略存储在一个名为“Registry.pol”

的 GPT 文件中；基于文件的 GPT 存储在每个域控制器的 Sysvol 文件夹中。

(3) 组策略容器组件

组策略容器组件是一个 AD 对象，列出了一个特定 GPO 关联的 GPT 名称。Windows 客户端使用一个 GPC 的信息来确定要下载和处理的 GPT 信息。

(4) 客户端扩展组件

在一个 Windows 客户端中有许多功能由组策略来管理。这些功能具备相应的服务，知道如何获取和处理指向它们的组策略。这些服务器被即客户端扩展组件 (Client Side Extension, CSE)，它以动态链接库的形式存在。

(5) 组策略编辑器组件

组策略编辑器组件 (Group Policy Editor, GPE) 是一个 MMC 管理单元，用于创建和管理 GPO。

(6) 计算机策略和用户策略组件

一个 GPO 的策略设置即可以用于计算机对象，也可以用于用户对象。计算机在启动时下载所属的策略，用户在登录到域控制器时下载所属的策略。

(7) 组策略和本地策略组件

并不是所有的策略都是从域中下载的，每个客户端都有自己的系列本地策略。如果用户不是一个域成员，那么在启动时将使用本地的策略，而不使用域策略。

➤➤ 3.7.2 组策略模板

在组策略编辑器的控制台展开“计算机配置”和“用户配置”分支，可以看到一个“管理模板”分支。其中提供了已定制的策略信息，用户可以根据需要启用或关闭策略。

1. 管理模板.adm 文件

.adm 文件是由类别和子类别组成的一种层次结构，这些类别和子类别共同定义了策略设置的显示方式。一个管理模板通常包括如下信息。

- (1) 每个设置对应的注册表位置。
- (2) 每个设置相关联的选项或对值的限制。
- (3) 策略默认值。
- (4) 每个设置的注释信息。
- (5) 支持每个设置的 Windows 版本。

Windows Server 2003 系统默认提供如下管理模板，分别用于实现不同的管理功能：

- (1) System.adm：系统设置模板。
- (2) Inetres.adm：Internet Explorer 设置模板。
- (3) Wmplayer.adm：Windows Media Player 设置模板，在 Windows Server 2003 家族 64 位版本中不可用。

- (4) Conf.adm：NetMeeting 设置模板，在 Windows Server 2003 家族 64 位版本中不可用。

- (5) Wuau.adm：Windows Update 设置模板。

2. Registry.pol 文件

组策略的管理模板扩展将信息保存在 Registry.pol 文件中，其中包括一些自定义的注册表设置，通过组策略指定的这些设置将被应用于注册表的计算机或用户部分。

- (1) Registry.pol 文件包含特定于 HKEY_LOCAL_MACHINE 项的注册表设置，它存储在 GPT\Machine 文件夹中。

- (2) Registry.pol 文件包含特定于 HKEY_CURRENT_USER 项的注册表设置，它存储在 GPT\User 子目录中。

3.7.3 通过组策略定制用户桌面

通过组策略可以为域用户定制具有特殊属性的桌面，在每一台成员计算机上登录时都会使用系统默认桌面。

① 登录到域控制器，打开“Active Directory 用户和计算机”窗口。新建一个组织单位，如 Office，将待部署安装程序的用户账户移动到该组织单位中。

② 单击“开始”→“管理工具”→“组策略管理”选项，显示如图 3-197 所示的“组策略管理”窗口，展开“组策略管理”→“林: coolpen.net”→“域”→“coolpen.net”→“book”选项。

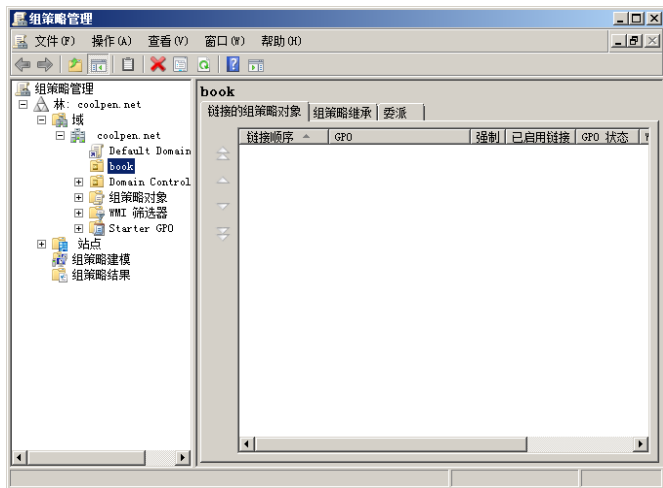


图 3-197 “组策略管理”窗口

③ 右击组织单位“book”，在快捷菜单中选择“在这个域中创建 GPO 并在此处连接”选项，显示如图 3-198 所示的“新建 GPO”对话框，在“名称”文本框中输入一个名称。



图 3-198 “新建 GPO”对话框

④ 单击“确定”按钮，创建完成一个组策略，如图 3-199 所示。

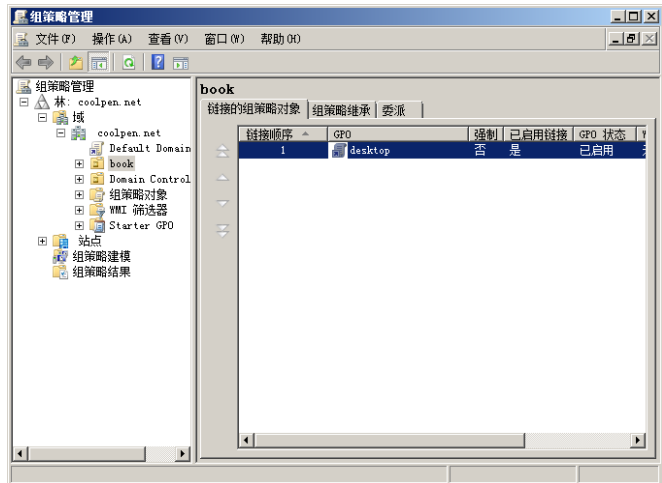


图 3-199 创建完成一个组策略

⑤ 右击组策略名称，选择快捷菜单中的“编辑”选项，打开如图 3-200 所示的“组策略管理编辑器”窗口。展开“用户配置”→“策略”→“管理模板”→“桌面”选项，在此处即可为用户定制桌面。

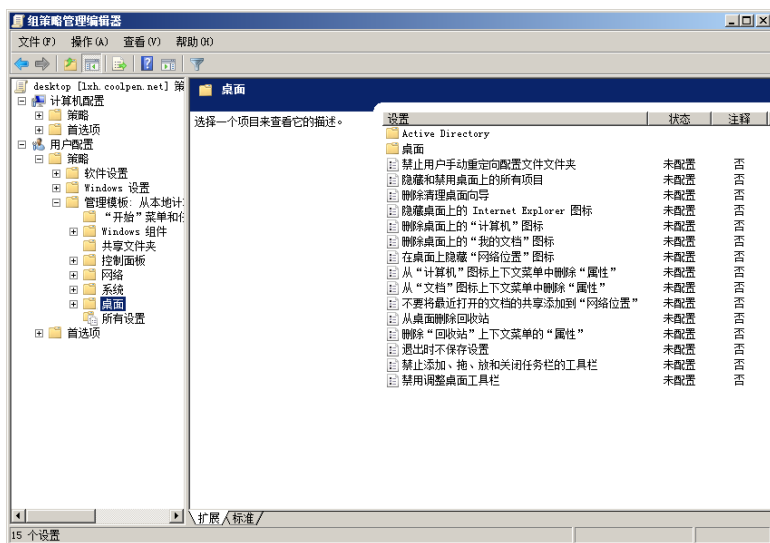


图 3-200 “组策略管理编辑器”窗口

以隐藏 IE 图标为例。双击“隐藏桌面上的 Internet Explorer 图标”选项，显示如图 3-201 所示的“隐藏桌面上的 Internet Explorer 图标 属性”对话框。选择“已启用”单选按钮，单击“确定”按钮。当用户在客户端计算机上登录时，将不会在桌面上显示 IE 图标。

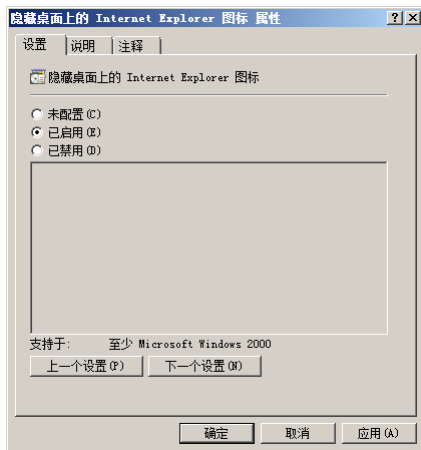


图 3-201 “隐藏桌面上的 Internet Explorer 图标 属性”对话框

根据实际需要，可以再为用户启用或禁用其他选项。当用户在客户端计算机登录以后，就会根据组策略中配置显示桌面。

3.7.4 通过组策略安装应用程序

在网络的多台计算机中安装相同软件，是一项非常麻烦的工作，需要在每台计算机上运行安装过程。如果计算机已加入域，则可以利用组策略同时为其部署安装应用程序，既方便又快捷。这里以部署 Office 2003 为例，在 Window Vista 系统中安装 Office。

1. 共享文件夹

在服务器上创建一个共享文件夹，将应用程序安装文件使用的 MSI 数据包复制到其中。

2. 配置客户端计算机

在客户端计算机上使用域用户模式登录 Windows Vista 系统, 启用“UAC”功能。默认设置 Windows Vista 操作系统关闭网络发现和文件共享功能, 需要启用该功能。

① 右击桌面右下角托盘区域的网络连接图标, 选择快捷菜单中的“网络和共享中心”选项, 显示如图 3-202 所示的“网络和共享中心”窗口。

② 在“共享和发现”选项组中单击“网络发现”右侧的按钮将其展开, 如图 3-203 所示。选择“启用网络发现”单选按钮, 单击“应用”按钮, 启用网络发现功能。



图 3-202 “网络和共享中心”窗口



图 3-203 展开“网络发现”

③ 单击“文件共享”右侧的按钮将其展开, 如图 3-204 所示, 选择“启用文件共享”单选按钮。

④ 单击“应用”按钮, 启用文件共享功能。然后启用公用文件夹共享功能, 如图 3-205 所示。



图 3-204 展开“文件共享”



图 3-205 启用公用文件夹共享

3. 创建部署策略

① 登录到域控制器, 打开“Active Directory 用户和计算机”窗口。新建一个组织单位, 如 Office, 将待部署安装程序的用户账户移动到该组织单位中。

② 单击“开始”→“管理工具”→“组策略管理”选项, 显示如图 3-206 所示的“组策略管理”窗口。选择“组策略管理”→“林: coolpen.net”→“域”→“coolpen.net”→“Office”选项。

③ 右击“Office”组织单位, 在快捷菜单中选择“在这个域中创建 GPO 并在此处连接”选项, 创建一个组策略。

④ 右击刚刚创建的组策略“安装 Office 2003”, 在快捷菜单中选择“编辑”选项, 打开“组策略

编辑管理器”窗口。展开“用户配置”→“策略”→“软件设置”→“软件安装”选项，如图 3-207 所示。

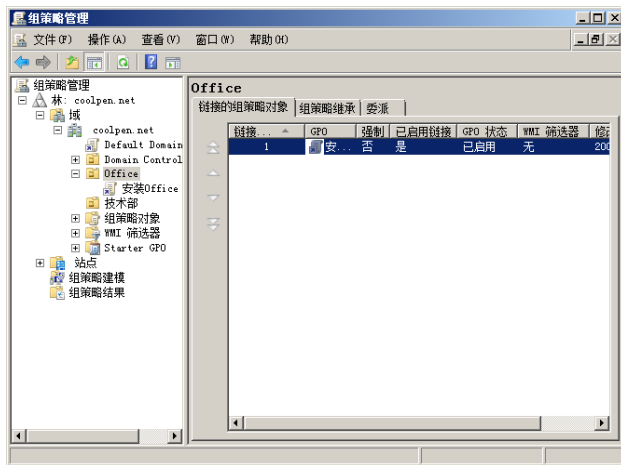


图 3-206 “组策略管理”窗口

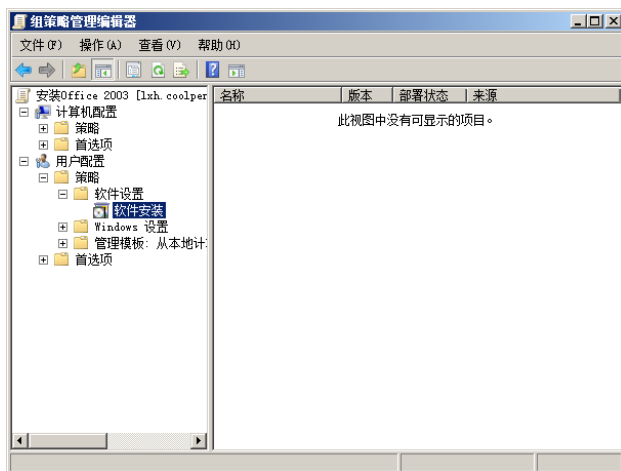


图 3-207 “软件安装”选项

⑤ 右击“软件安装”选项，选择快捷菜单中的“新建”→“数据包”选项。显示如图 3-208 所示的“打开”对话框，在 Office 共享文件夹中选择安装程序。

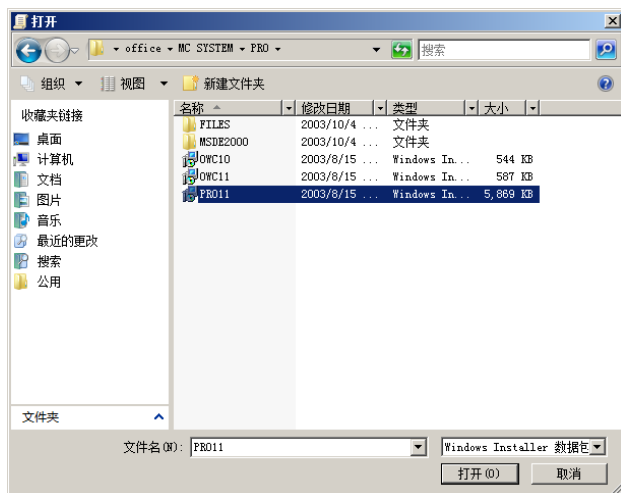


图 3-208 “打开”对话框

**提示**

文件路径必须是网络路径，共享文件位置可以位于网络上任何一台计算机，但是必须具备足够的访问权限。

⑥ 单击“打开”按钮，显示如图 3-209 所示的“部署软件”对话框。

在其中的选择软件部署的如下方法。

- 已发布：当软件分发给用户且组策略生效后，用户在任何一台计算机登录，所部署的软件都将显示在“添加/删除程序”对话框中。但此时并没有真正安装，需要用户手动安装在所使用的计算机上。
- 已分配：当软件分配给计算机时，计算机在下次启动时自动下载并安装软件。用户登录以后即可使用，但不能删除该软件；除非具备管理员权限。

⑦ 单击“确定”按钮，软件部署完成，如图 3-210 所示。

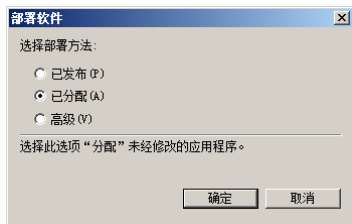


图 3-209 “部署软件”对话框

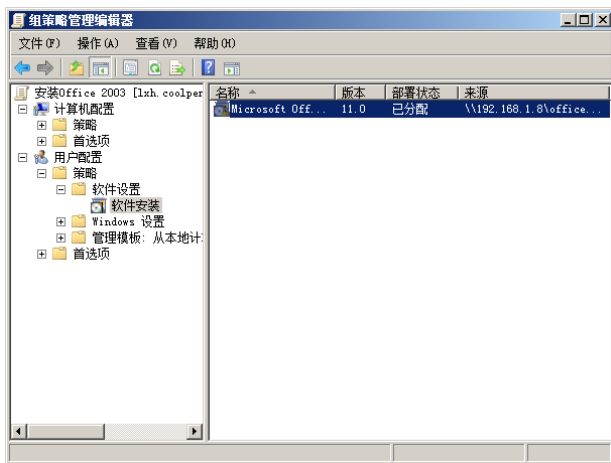


图 3-210 软件部署完成

⑧ 右击新建的数据包，在快捷菜单中选择“属性”选项。显示属性对话框，默认为如图 3-211 所示的“常规”选项卡。

⑨ 打开如图 3-212 所示的“部署”选项卡，在“部署选项”选项组中选中“在登录时安装此应用程序”复选框当用户登录到 Active Directory 时将自动安装应用程序。

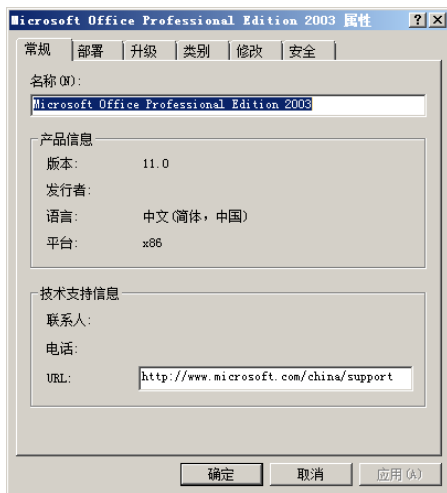


图 3-211 “常规”选项卡

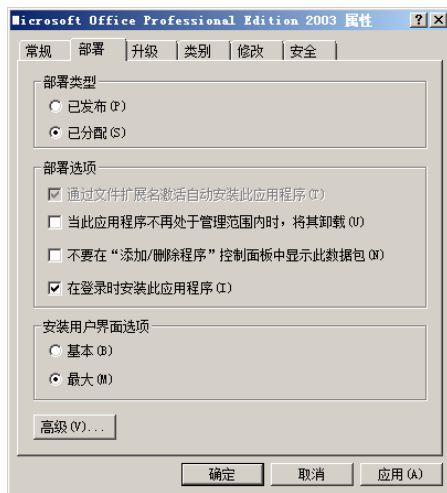


图 3-212 “部署”对话框

⑩ 单击“确定”按钮，创建完成软件部署策略。

4. 测试客户端

在客户端计算机上以域用户账户身份登录，系统会在后台自动通过组策略安装 Office 2003。安装完成后进入 Windows Vista 操作系统，打开“开始”菜单，选择“Microsoft Office”选项即可显示安装的 Office 程序列表，如图 3-213 所示。



注意：

如果 Office 安装程序没有配置应答文件在安装时自动输入序列号，那么当域用户打开 Office 应用程序时，就会显示如图 3-214 所示的安装界面，提示输入产品密钥。

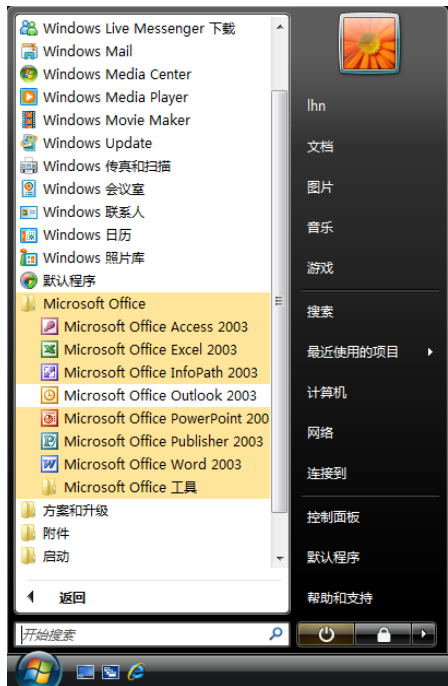


图 3-213 Office 安装列表

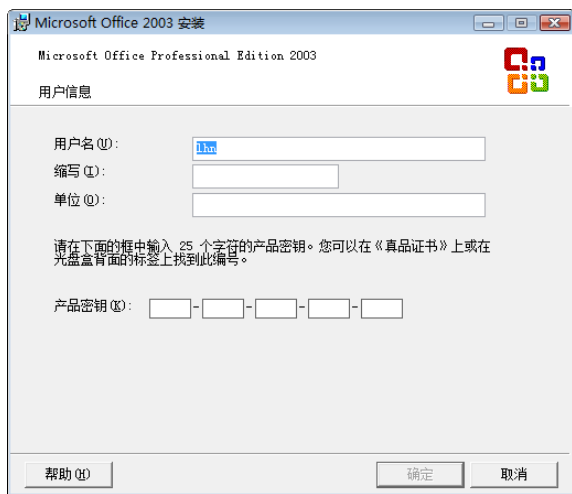


图 3-214 Office 安装界面

3.8 Windows 客户端加入域

客户端计算机必须先添加入域，才能使用用户账户登录到域，接受域的统一管理并且使用域中的资源。目前的 Windows 系列操作系统中，除 Home 版的操作系统外都可以添加到域，如 Windows 2000 Professional、Windows XP Professional、Windows Vista 及 Windows Server 2003/2008 等。需要注意的是，在添加到域之前，应该将客户端计算机的 DNS 地址设置为域控制器的 IP 地址。

3.8.1 Windows 2000 Professional 用户

操作步骤如下。

- ① 右击桌面上的“我的电脑”图标，显示“系统特性”对话框。打开“网络标识”选项卡，如图 3-215 所示。
- ② 单击“属性”按钮，显示如图 3-216 所示的“标识更改”对话框。在“隶属于”选项组中选择“域”单选按钮，并键入域名。
- ③ 单击“确定”按钮，显示如图 3-217 所示的“域用户名和密码”对话框，在“名称”和“密码”文本框中分别输入具有加入域权限的用户名和密码。
- ④ 单击“确定”按钮，显示如图 3-218 所示的“网络标识”对话框，提示加入域成功。

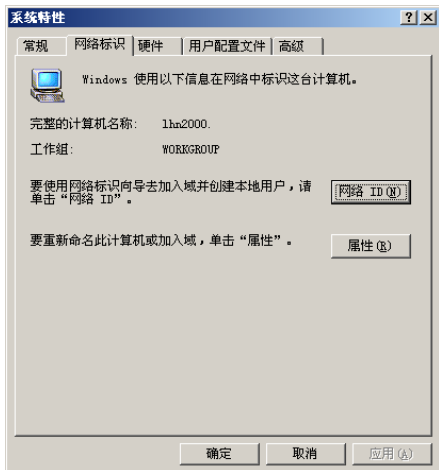


图 3-215 “网络标识”选项卡

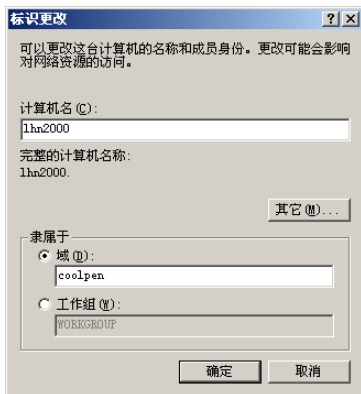


图 3-216 “标识更改”对话框

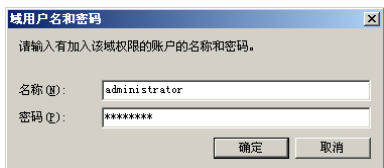


图 3-217 “域用户名和密码”对话框



图 3-218 “网络标识”对话框

- ⑤ 单击“确定”按钮，显示如图 3-219 所示的提示框，提示必须重新启动计算机才能使更改生效。
- ⑥ 单击“确定”按钮，显示如图 3-220 所示的“系统设置改变”对话框，提示现在是否要重新启动计算机。



图 3-219 提示框



图 3-220 “系统设置改变”对话框

- ⑦ 单击“是”按钮重新启动计算机。当显示如图 3-221 所示的“登录到 Windows”界面时，单击“选项”按钮。在“登录到”下拉列表框中选择待登录的域名，在“用户名”和“密码”文本框中分别输入具有登录域权限的用户账户名和密码。
- ⑧ 单击“确定”按钮，即可登录到域。



图 3-221 “登录到 Windows”界面

3.8.2 Windows XP Professional 用户

操作步骤如下。

- ① 使用具有管理员权限的账户登录系统，右击“我的电脑”图标。选择快捷菜单中的“属性”

选项，显示“系统属性”对话框，打开“计算机名”选项卡，如图 3-222 所示。

② 单击“更改”按钮，显示如图 3-223 所示的“计算机名称更改”对话框。选择“域”单选按钮，并输入域名。

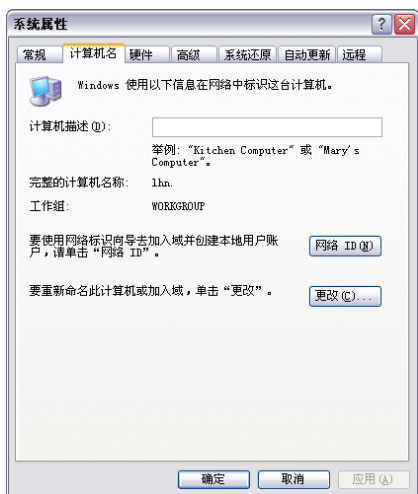


图 3-222 “计算机名”选项卡

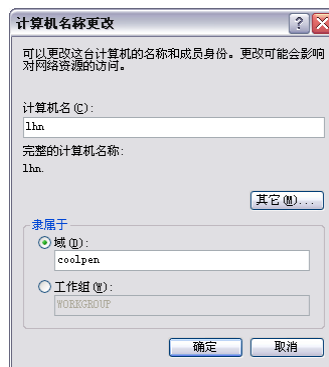


图 3-223 “计算机名称更改”对话框

③ 单击“确定”按钮，显示如图 3-224 所示的“计算机名更改”对话框，在“用户名”和“密码”文本框中输入具有加入域权限的用户账户和密码。

④ 单击“确定”按钮即可连接域控制器并加入，显示如图 3-225 所示的提示框，提示欢迎加入域。



图 3-224 “计算机名更改”对话框



图 3-225 提示框

⑤ 单击“确定”按钮，并根据系统提示重新启动计算机。当显示如图 3-226 所示的“登录到 Windows”对话框时，单击“选项”按钮。在“登录到”下拉列表框中选择域名，并在“用户名”和“密码”文本框中输入具有登录域权限的用户账户和密码即可。



图 3-226 “登录到 Windows”对话框

⑥ 单击“确定”按钮即可登录到域。

3.8.3 Windows Vista 用户

将 Windows Vista 计算机加入域以后,在使用域用户账户登录域时不能直接输入用户账户名,而应使用“域名\用户账户”的格式。

① 打开“开始”菜单,右击“计算机”选项。选择快捷菜单中的“属性”选项,显示如图 3-227 所示的“系统”窗口。



图 3-227 “系统”窗口

② 在“计算机名称、域和工作组设置”选项组中单击“改变设置”超级链接,显示“系统属性”对话框。在“计算机名”选项卡中单击“更改”按钮,打开如图 3-228 所示的“计算机名/域更改”对话框。选择“域”单选按钮,并输入待加入的域名。

③ 单击“确定”按钮,显示如图 3-229 所示的“Windows 安全”对话框,要求输入具有加入域权限的用户名和密码。

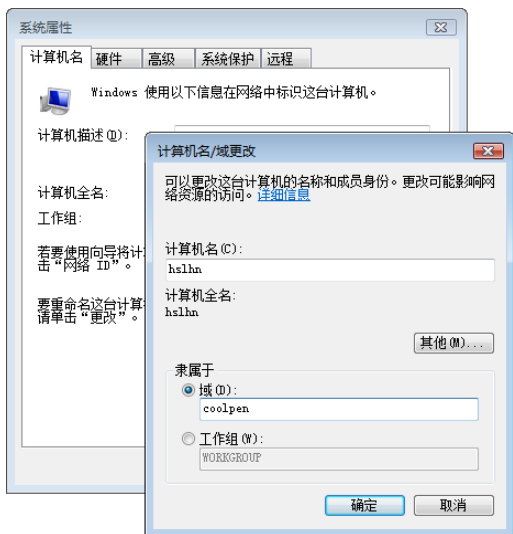


图 3-228 “计算机名/域更改”对话框

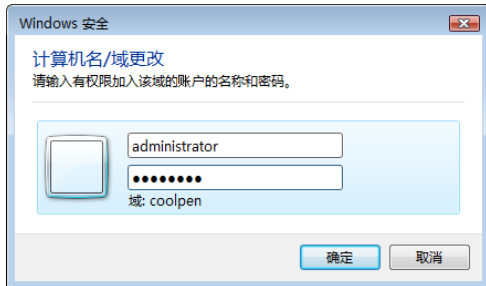


图 3-229 “Windows 安全”对话框

④ 单击“确定”按钮,显示如图 3-230 所示的提示框,提示加入域成功。操作过程中建议关闭本地计算机的各种防火墙软件,以免导致操作失败。

⑤ 单击“确定”按钮，根据系统提示重新启动计算机。当启动到登录界面以后，单击“切换用户”按钮，显示选择用户界面。单击“其他用户”按钮，显示如图 3-231 所示的登录界面。在“用户名”文本框中输入待登录的域用户账户，例如 coolpen\lhn，并在“密码”文本框中输入账户密码。



图 3-230 提示框



图 3-231 登录界面

⑥ 按回车键即可登录到域。

第 4 章 WINS 服务

在 TCP/IP 网络中，计算机之间必须使用名称解析的方式通过主机名找到对应的 IP 地址，以利用 IP 地址通信。WINS（Windows Internet Name Service，Windows Internet 命名服务）提供名称解析功能，其客户端会向 WINS 服务器注册，将计算机名与对应的 IP 地址添加到 WINS 服务器的数据库中。从而使得其他计算机可以从 WINS 服务器中获得对方的 IP 地址，完成名称解析过程并通信。由于 IP 地址的解析工作由 WINS 服务器完成，因此大幅度地减少了网络管理员的工作量。

4.1 WINS 服务器概述

WINS 是微软提供的名称解析服务，不仅可以在 TCP/IP 网络中为同一网段提供名称解析服务，也可以为不同网段的计算机提供解析功能。使网络中的计算机不需知道对方的 IP 地址，只需利用计算机名即可在 WINS 服务器上查询到相应的 IP 地址，从而实现通信。

4.1.1 WINS 简介

早期的 Windows 9x/NT 等操作系统在进行 IP 地址解析时都使用 HOSTS 文件，而该文件的工作基础是 NetBIOS。NetBIOS 需要广播大量的网络资源信息，虽然可以使网络中的任何客户端都能够接收到，但是在较大型的网络中广播信息不仅会产生大量的无用信息，还占用大量的网络带宽和计算机处理时间。有时还会产生广播风暴，影响网络的正常通信。另外，NetBIOS 信息是不可路由的。广播信息只能在一个网段内传输，无法传到其他网段。鉴于这些缺点，微软提供了基于 TCP/IP 协议栈的 NetBIOS（即 NBT）。NBT 可以路由，并且仍以广播方式工作，这就是 WINS。

当 WINS 客户端启动时，会向 WINS 服务器发送 NBT 广播信息。WINS 服务器监听到该信息后会自动将该 WINS 客户端的计算机名称（即 NetBIOS 名）与对应的 IP 地址等信息添加到 WINS 数据库中，完成 WINS 服务器注册。由于 WINS 客户端每次启动时都要向 WINS 服务器注册一次，因此 WINS 服务器的数据库总是在不断地更新的，以确保 WINS 客户端永远能够享受 WINS 服务器提供的服务。如果网络的规模较大，可以在网络中设置多台 WINS 服务器，将查询和应答操作分配给多台 WINS 服务器进行分布式处理，从而提高网络效率。

由于 WINS 客户端之间需要通过 IP 地址通信，所以需要先向 WINS 服务器查询计算机名称对应的 IP 地址。当 WINS 服务器收到客户端的请求后，就会自动从本地数据库中查找与计算机名对应的 IP 地址，并提供给客户端完成解析过程。

WINS 的解析方式与 DNS 有些类似，但又完全不同。DNS 系统建立一种主机名与 IP 地址之间的映射关系，即由主机名来查找其 IP 地址（也可以通过反向查寻方式由 IP 地址找到其主机名）。而 WINS 服务器会同时提供对方的计算机名和 IP 地址，不存在名称与 IP 地址之间的映射关系。

WINS 在工作中要经过以下 3 个步骤。

（1）每一台 WINS 客户端在启动时都会将其计算机名和 IP 地址在 WINS 服务器中注册，通知 WINS 服务器有一台 WINS 客户端加入网络。

（2）当两台 WINS 客户端要建立通信时，解析对方计算机名和 IP 地址的查询将直接发送到 WINS 服务器，而不是以广播方式送往整个网络。

（3）当 WINS 服务器在数据库中找到了对应的计算机名和 IP 地址，则直接返回给 WINS 客户端；如果没有找到，WINS 服务器就产生一个标准的 NBT 广播来寻找需要的地址。



在 Windows NT 4.0 和更早版本的域中必须使用 NetBIOS 名，在 Windows Server 2000/2003/2008 系统中活动目录域依靠 DNS 进行名称解析，已经不再需要 NetBIOS 和 WINS 服务器。只是为了兼容早期的 Windows，仍支持 WINS 服务。通常情况下，用户不必配置 WINS 服务器。

4.1.2 WINS 的工作机制

WINS 客户端可以在启动时向指定的 WINS 服务器注册，通常一台 WINS 客户端可以指定两台 WINS 服务器，即主 WINS 服务器和辅助 WINS 服务器。当主 WINS 服务器无法为 WINS 客户端提供服务时，可以由辅助 WINS 服务器继续提供服务。WINS 的工作机制可以分为 4 个阶段，即名称注册、名称续租、名称释放和名称解析。

1. 名称注册

在 WINS 系统中，WINS 客户端启动时可以利用点对点的方式直接与 WINS 服务器建立连接，以便将其计算机名和 IP 地址等信息注册到 WINS 服务器中。而当 WINS 服务器在收到一个注册请求时，还要根据数据库中是否存在该数据来判断是否要接受该 WINS 客户端的注册请求。具体地讲，当 WINS 服务器接收到 WINS 客户端的请求后，还需要执行以下操作。

(1) 判断名称是否唯一

由于网络中的计算机可能会存在同名，所以一个计算机名可能会已被注册过。此时另一台也使用此名称的客户端向 WINS 服务器注册时，WINS 服务器经检查发现数据库中已有该名称，就会向拥有该名称且已注册的计算机发出一个询问信息，其结果有两种可能。

- 如果已注册了该名称的计算机发出响应，WINS 服务器便向试图使用该名字注册的 WINS 客户端发出一个否定信息，告诉它不能够使用此名称注册。
- 如果已注册了该名称的计算机没有响应，则 WINS 服务器会连续发送 3 次该查询信息，每次的间隔时间为 500 ms。如果经过连续 3 次查询仍无反应，就会从数据库中删除该名称。并向请求注册的 WINS 客户端发出肯定回答，接受其注册请求。

(2) 判断名称是否有效

如果计算机名中含有非法字符，则 WINS 服务器将拒绝接受注册。NetBIOS 名称的命名有如下严格规定。

- 长度不能超过 15 个半角字符。
- 只能使用字母 a~z、数字 0~9 和连线“-”。
- 不能包含特殊字符（如“？”及“/”等）。

2. 名称续租

在 WINS 系统中，WINS 客户端需要不断地告诉 WINS 服务器要继续使用已注册的名称。这样 WINS 服务器才会更新 WINS 客户端的名称租期，重新复位 TTL (Time To Live, 生存时间)。

WINS 的续租方式和 DNS 类似，当 TTL 到达预设值的一半时间时，WINS 客户端会向其主 WINS 服务器发送一个续租请求信息，包括该 WINS 客户端的计算机名称、源 IP 地址（该 WINS 客户端的 IP 地址）和目的 IP 地址（已注册 WINS 服务器的 IP 地址）。如果主 WINS 服务器没有反应，该请求信息在 TTL 剩余 1/8 的时刻重发一次；如果主 WINS 服务器仍无反应，并且网络中配置有辅助 WINS 服务器，则该 WINS 客户端将尝试向辅助 WINS 服务器续租。

如果辅助 WINS 服务器接收续租，WINS 客户端就在辅助 WINS 服务器获得一个 TTL；如果向辅助 WINS 服务器发送了 3 次续租请求后，仍然没有得到辅助 WINS 服务器的回应，则该 WINS 客户端又继续向主 WINS 服务器请求续租。该过程将一直继续下去，直到得到 WINS 服务器的响应为止。

3. 名称释放

如果 WINS 客户端需要释放名称，可以随时向 WINS 服务器发送一个包含 IP 地址和计算机名的名

称释放信息，以放弃名称拥有权。当 WINS 服务器收到一个释放信息后，将从数据库中删除该 WINS 客户端的注册信息，并返回一个确认释放信息和一个值为 0 的 TTL。此时，该 WINS 客户端在 WINS 服务器中已没有任何注册信息了，这种情况主要在 WINS 客户端关机时进行。

4. 名称解析

在 Microsoft 网络中，当两台 WINS 客户端之间需要建立通信关系时，除了使用 WINS，还可以利用广播或 LMHOSTS 文件两种方式。也可以同时使用 3 种方式，以解决名称解析问题。这 3 种方式可用如下 4 种模式来配合。

(1) b-节点 (b-node)

该模式使用广播方式来查找 IP 地址。例如，当计算机 A 要与计算机 B 通信时，计算机 A 就会向网络中发送一个寻找计算机 B 的信息，然后就等待计算机 B 的回应。当计算机 B 收到该寻找信息后，就会将自己的 IP 地址发送给计算机 A。当计算机 A 收到计算机 B 的 IP 地址后，就可以建立与计算机 B 的联系。

很显然，广播方式的工作原理非常简单，但是会增加网络的负担。而且无法跨网段操作，因为路由器无法将这种广播信息转发给下一个网段。

(2) p-节点 (p-node)

该模式使用点对点的工作方式，直接向 WINS 服务器查询计算机的 IP 地址。例如，当计算机 A 要与计算机 B 通信时，计算机 A 将直接向 WINS 服务器查询。然后由 WINS 服务器将计算机 B 的 IP 地址提供给计算机 A，从而建立计算机 A 与计算机 B 之间的联系。

(3) m-节点 (m-node)

该模式是 b-节点与 p-节点两种模式的结合，它首先使用 b-节点的广播方式。如果该方式失败，则转而使用 p-节点方式向 WINS 服务器查询。例如，当计算机 A 要与计算机 B 通信时，计算机 A 先利用广播方式查找计算机 B 的 IP 地址。如果计算机 B 没有反应（如其位于另一个网段），则使用点对点的方式在 WINS 服务器中查询。

(4) h-节点 (h-node)

h-节点 (hybrid-node) 的工作过程与 m-节点模式正好相反，该模式首先使用点对点方式向 WINS 服务器查询。如果失败，则转向使用广播方式。例如，当计算机 A 要与计算机 B 通信时，计算机 A 先向 WINS 服务器查询。如果 WINS 服务器无法提供计算机 B 的 IP 地址，则改用广播方式在该网段内查找计算机 B。

除以上的 4 种方式外，Windows 网络系统的 b-节点模式还提供另外一种扩充功能，即 extended b-node。当利用广播模式失败后，则尝试在 LMHOSTS 文件中查找是否有要与之通信的计算机名称和对应的 IP 地址。由于该文件可以记录其他网段内的 IP 地址，所以可以克服无法跨网段传输的缺点。Microsoft 网络系统默认的名称解析方式是 b-节点广播方式，但如果是 WINS 客户端，则默认使用 h-节点模式。在 Windows 系统中，可以使用 ipconfig /all 命令来查看计算机目前所采用的模式，如图 4-1 所示。

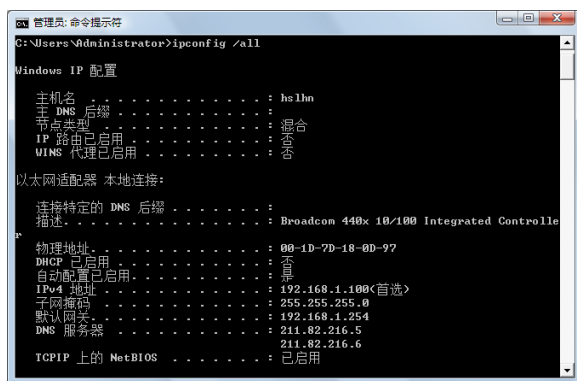


图 4-1 查看计算机目前所采用的模式

4.2 WINS 服务器的配置与管理

WINS 服务是 Windows Server 2003 和 Windows Server 2008 系统自带的功能，可以为网络中的 WINS 客户端提供名称解析。即使是不同网段中的非 WINS 客户端，也可以通过配置静态映射功能，使不同计算机之间可以相互通信。

4.2.1 安装 WINS 服务器

Windows Server 2008 操作系统安装完成后，默认并没有安装 WINS 服务，需要网络管理员运行“添加功能向导”来安装 WINS 服务器。

① 在“初始配置任务”或“服务器管理器”窗口中单击“添加功能”超级链接，启动“添加功能向导”。选中“WINS 服务器”复选框，如图 4-2 所示。

② 单击“下一步”按钮，显示如图 4-3 所示的“确认安装选择”对话框。

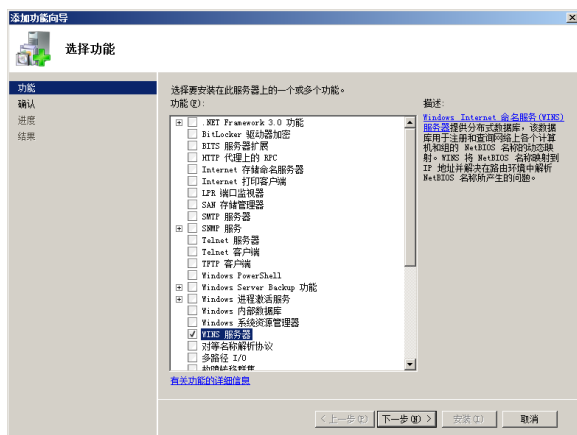


图 4-2 选中“WINS 服务器”复选框



图 4-3 “确认安装选择”对话框

③ 单击“安装”按钮，开始安装。完成后显示如图 4-4 所示的“安装结果”对话框，提示 WINS 服务器安装成功。

④ 单击“关闭”按钮，在“服务器管理器”控制台中依次展开“功能”→“WINS”选项。即可看到已安装的 WINS 服务，如图 4-5 所示。

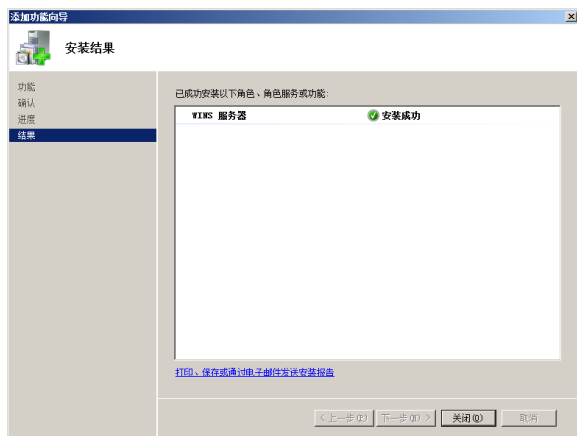


图 4-4 “安装结果”对话框

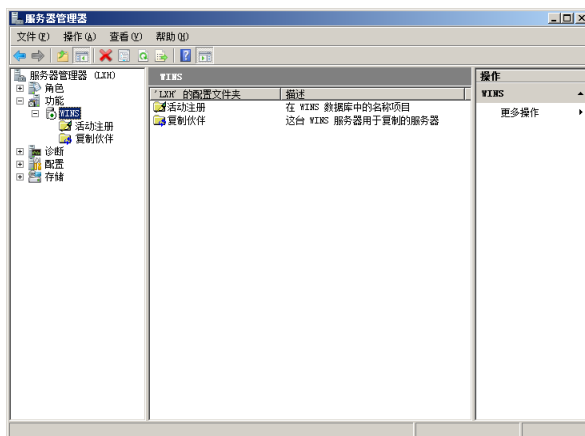


图 4-5 已安装的 WINS 服务

4.2.2 静态映射

由于非 WINS 客户端不会自动在 WINS 服务器中注册，所以 WINS 服务器的数据库中也没有非其计

算机名和 IP 地址。当支持和不支持 WINS 服务的客户端位于同一网段时，相互之间可以利用广播方式寻找；如果位于不同网段，由于广播信息不可路由，无法从一个网段转发到另一个网段。因此 WINS 客户端无法与非 WINS 客户端通信，需要利用静态映射功能在 WINS 服务器中手动添加非 WINS 客户端。

1. 添加静态映射

利用静态映射功能，可以手动将网络中非 WINS 客户端的计算机名和 IP 地址添加到 WINS 服务器的数据库中，这些数据也称为“静态映射数据”。当在 WINS 服务器的数据库中创建静态映射数据后，可以供非 WINS 客户端查询。创建静态映射数据的方法如下。

① 打开“服务器管理器”窗口，依次展开“功能”→“WINS”→“活动注册”选项，右击“活动注册”选项。并选择快捷菜单中的“新建静态映射”选项，显示如图 4-6 所示的“新建静态映射”对话框。

② 在“计算机名”和“IP 地址”文本框中分别输入非 WINS 客户端的计算机名和 IP 地址。在“类型”下拉列表框中可选择所添加的该静态映射数据的类型，其中包含的选项及其意义如下。

- 唯一：将计算机名与 IP 地址设置为一对一的关系。
- 组：指该静态映射数据是一个组，其中 WINS 服务器的数据库并不会存储该组内用户的信息（计算机名和 IP 地址）。当 WINS 服务器收到非 WINS 客户端的查询请求时，将会为该客户端提供一个 255.255.255.255 的广播地址。
- 域名：指该静态映射数据是一个域控制器的组，其中“IP 地址”中输入的应该是该组的域控制器的 IP 地址。
- Internet 组：这是一个用户自定义的组，可以将其他资源组成一个组，以提供给客户端查询（访问）。一个 Internet 组中最多可以设置和存储 25 个地址。
- 多主：同一个计算机名可以对应多个 IP 地址，这种方式用于在同一台计算机中安装多块网卡，或者一块网卡绑定了多个 IP 地址的情况。

③ 设置完成后，单击“应用”按钮添加成功。可继续添加其他非 WINS 客户端。最后单击“确定”按钮返回 WINS 窗口。

2. 查看 WINS 服务器中的注册信息

在 WINS 服务器中添加数据以后，默认并不会显示在 WINS 控制台中，可以执行以下步骤来查看注册信息。

① 在“服务器管理器”窗口中依次展开“功能”→“WINS”选项，右击“活动注册”选项。选择快捷菜单中的“显示记录”选项，显示如图 4-7 所示的“显示记录”对话框。如果添加的数据比较多，可以设置筛选条件。

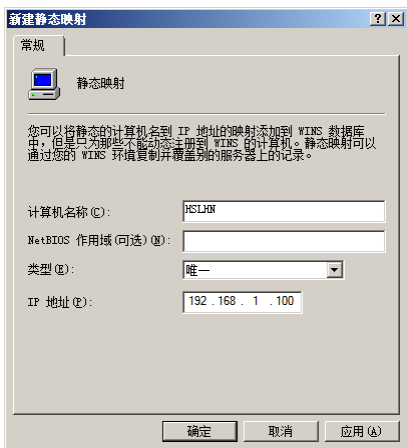


图 4-6 “新建静态映射”对话框

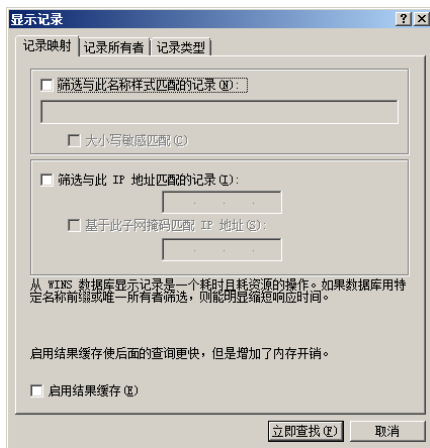


图 4-7 “显示记录”对话框

- ② 单击“立即查找”按钮，显示 WINS 数据库中的所有记录，如图 4-8 所示。

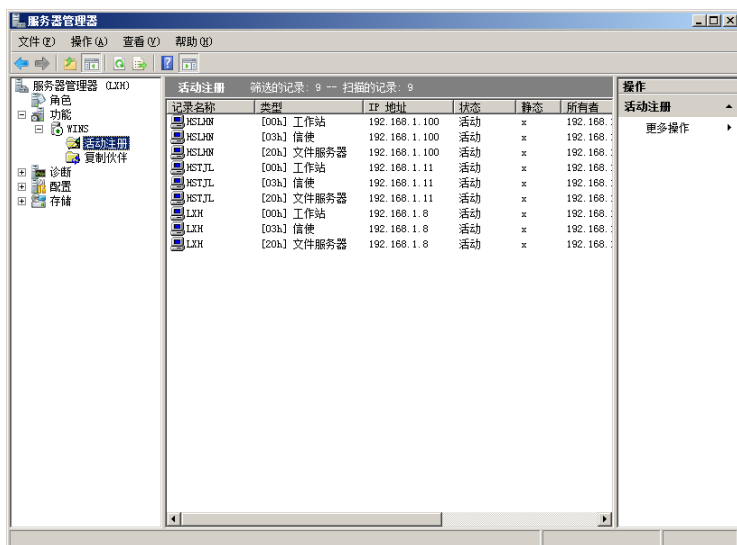


图 4-8 WINS 数据库中的所有记录

4.2.3 复制配置

在网络中一般在每个网段中设置一台 WINS 服务器来提供注册和查询等服务，使同一网段中的 WINS 客户端可以相互通信。如果有多个网段，为了使不同网段中的 WINS 客户端能相互通信，需要在不同网段中的 WINS 服务器之间进行复制。使每一台 WINS 服务器中都有其他网段的 WINS 数据库中的记录，从而保证任意网段的 WINS 客户端之间都能够通信。

1. 新建复制伙伴

复制伙伴是指 WINS 服务器之间进行复制数据库时所确立的一种关系，根据处理数据库方式的不同又分为“推伙伴”和“拉伙伴”。

(1) 推伙伴：将当前 WINS 服务器中的数据复制到另一台 WINS 服务器中时，对当前 WINS 服务器来说，所建立的复制伙伴关系就是推伙伴。所谓推，即指将自己数据库中的数据记录复制给其他 WINS 服务器。

(2) 拉伙伴：将当前 WINS 服务器中的数据复制到另一台 WINS 服务器中时，对目标 WINS 服务器来说，所建立的复制关系是拉伙伴。所谓拉，即指接收对方 WINS 服务器中的数据记录。

推伙伴和拉伙伴是同一个过程的两个方面，任何 WINS 服务器的复制过程都会同时存在推伙伴和拉伙伴。WINS 服务器数据库之间的复制过程在以下两种条件下激发。

- (1) 已到达系统管理员所设置的复制时间。
- (2) 用手动方式向系统发出复制操作命令。

提示



两台服务器进行复制时，一台设置为“推伙伴”，那么另一台必须设置为“拉伙伴”；否则无法复制和接收数据。另外，如果要实现两台 WINS 服务器之间数据的相互复制，则必须互相设置为“推伙伴”和“拉伙伴”。

复制 WINS 服务器的过程如下。

① 在“服务器管理器”窗口中依次展开“功能”→“WINS”→“复制伙伴”选项，右击“复制伙伴”选项。在快捷菜单中选择“新建复制伙伴”选项，显示如图 4-9 所示的“新的复制伙伴”对话框，在“WINS 服务器”文本框中输入另一台 WINS 服务器的名称或 IP 地址。

② 单击“确定”按钮，已创建的复制伙伴显示在 WINS 窗口中，如图 4-10 所示，并且该复制伙

伴的关系系统默认设置为“推”/“拉”。

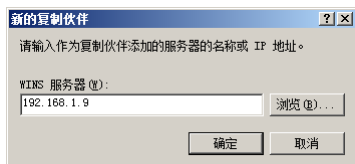


图 4-9 “新的复制伙伴”对话框

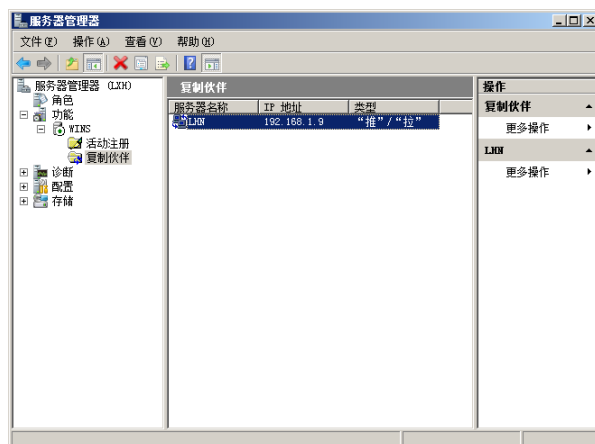


图 4-10 已创建的复制伙伴显示在 WINS 窗口中

创建一个复制伙伴后，还可以对其进行必要的设置。在 WINS 服务器窗口中选择已创建的复制伙伴，右击并从快捷菜单中选择“属性”选项，显示其属性对话框。切换到“高级”选项卡，如图 4-11 所示，可在其中设置以下选项。

- 复制伙伴类型：设置该 WINS 服务器是“推”或“拉”或者“推”/“拉”。

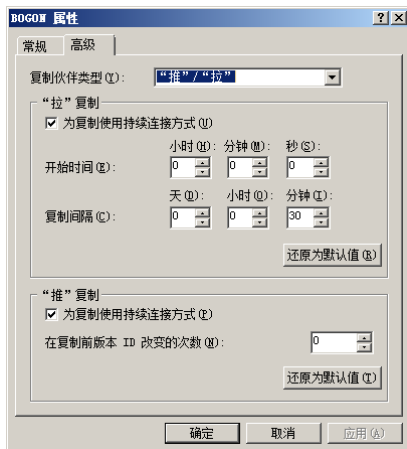


图 4-11 “高级”选项卡

- “拉”复制：如果选中“为复制使用持续连接方式”复选框，则在复制过程中与“拉伙伴”一起使用持续连接。当 WINS 服务器之间的复制完成后，保持连接不中断。以便下次复制时直接使用，减少时间的浪费及网络负担；“开始时间”设置每天开始复制的时间，建议设置为网络工作的空闲时间；“复制间隔”用于设置每隔多长时间复制一次。
- “推”复制：“为复制使用持续连接方式”的功能与“拉”复制相同；“在复制前版本 ID 改变的次数”用于设置当 WINS 数据库改变了多少条数据后开始复制操作，WINS 数据库中的每一条记录都拥有一个版本 ID。

2. 手动复制

WINS 服务器既可设置自动复制，也可以利用手动复制方式立即复制数据库。手动复制包括“开始‘推’复制”和“开始‘拉’复制”两种，其中“开始‘推’复制”表示立即将数据复制给对方 WINS 服务器；“开始‘拉’复制”则表示立即向对方 WINS 服务器要求复制数据，并执行复制操作。

手动复制的操作方法如下。

① 打开 WINS 窗口，选择复制伙伴。右击并从快捷菜单中选择复制方式，如“开始‘推’复制”选项，显示如图 4-12 所示的“启动‘推’复制”对话框。

根据需要选择如下复制方式。

- 仅为伙伴启动：仅将数据复制到已选择的对方 WINS 服务器中。
- 传播到所有伙伴：将数据复制到所有与该 WINS 服务器建立复制伙伴关系的 WINS 服务器中。

② 选择一种复制方式后，单击“确定”按钮显示如图 4-13 所示的提示框，单击“确定”按钮完成复制操作。

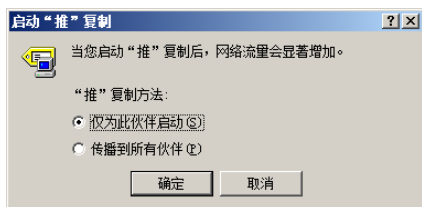


图 4-12 “启动‘推’复制”对话框

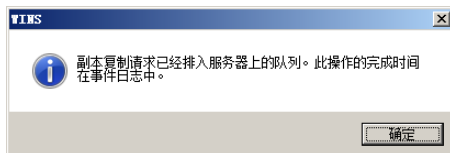


图 4-13 提示框

4.2.4 备份与还原 WINS 服务器

1. 备份

为防止 WINS 服务器出现故障，可事先备份 WINS 服务器数据库中的数据以便日后还原，操作步骤如下。

① 在“服务器管理器”窗口中打开 WINS 控制台，右击 WINS 服务器名称。选择快捷菜单中的“备份数据库”选项，显示如图 4-14 所示的“浏览文件夹”对话框，选择一个保存备份数据的路径。

② 单击“确定”按钮备份数据库，显示如图 4-15 所示提示框。提示数据库备份成功，单击“确定”按钮即可。

2. 还原

在还原 WINS 数据库之前，必须首先停止 WINS 服务；否则无法还原，并且“还原数据库”选项为不可用状态。

① 右击 WINS 服务器名称，选择快捷菜单中的“所有任务”→“停止”选项，停止 WINS 服务器。

② 右击 WINS 服务器名称，选择快捷菜单中的“还原数据库”选项，显示“浏览文件夹”对话框。选择保存数据库备份的文件夹，单击“确定”按钮还原，并显示如图 4-16 所示的提示框。

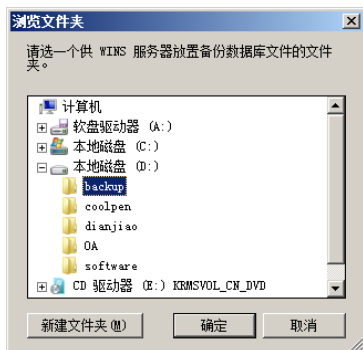


图 4-14 “浏览文件夹”对话框



图 4-15 数据库备份成功



图 4-16 提示框

③ 单击“确定”按钮，WINS 数据库还原成功，并且 WINS 服务器会自动启动。

4.3 设置 WINS 客户端

WINS 服务器安装并配置完成以后,需要在 WINS 客户端中配置其地址才可使用 WINS 服务。通常可以利用 DHCP 服务器分配 IP 地址的方式来配置 WINS 服务地址,也可以利用手动的方法在 WINS 客户端中添加该地址。

4.3.1 在 DHCP 服务器中分配 WINS 服务器地址

如果网络中使用 DHCP 服务器分配 IP 地址,可在 DHCP 作用域中设置 WINS 服务器,使 DHCP 客户端在获得 IP 地址时可获得并配置 WINS 服务器地址。

当使用“添加角色向导”安装 DHCP 服务器时,可以显示如图 4-17 所示的“指定 IPv4 WINS 服务器设置”对话框时选择“此网络上的应用程序需要 WINS”单选按钮,并在“首选 WINS 服务器 IP 地址”和“备用 WINS 服务器 IP 地址”文本框中键入 WINS 服务器的 IP 地址。

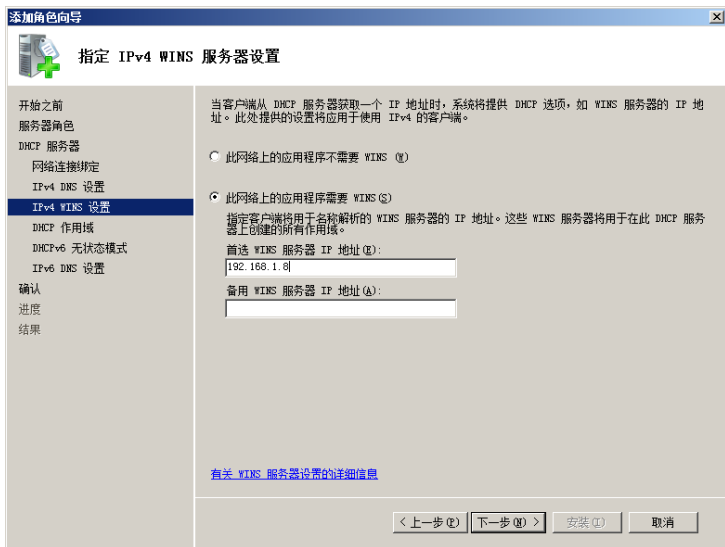


图 4-17 “指定 IPv4 WINS 服务器设置”对话框

在 DHCP 服务器中新建作用域时,当显示如图 4-18 所示的“WINS 服务器”对话框时在“服务器名称”文本框中输入 WINS 服务器名称,单击“解析”按钮解析出 IP 地址。或者直接在“IP 地址”文本框中键入 WINS 服务器的 IP 地址,单击“添加”按钮添加到列表框中即可。

这样当客户端从 DHCP 服务器获得 IP 地址时,会同时获得 WINS 服务器地址。

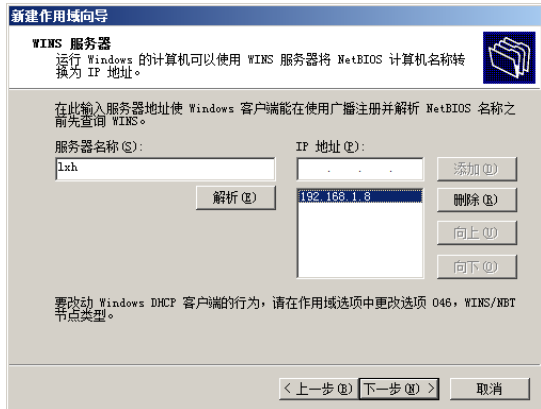


图 4-18 “WINS 服务器”对话框

4.3.2 客户端配置

网络中的客户端计算机需要添加 WINS 服务器的 IP 地址,才能使用 WINS 服务器来解析计算机名与 IP 地址。常用的 WINS 客户端操作系统主要有 Windows XP 和 Windows Vista。

1. Windows XP 设置

- ① 通过“控制面板”打开“网络连接”窗口,右击“本地连接”并从快捷菜单中选择“属性”选项,显示“本地连接 属性”对话框。
- ② 选择“Internet 协议 (TCP/IP)”选项,单击“属性”按钮,显示“Internet 协议(TCP/IP) 属性”对话框。单击“高级”按钮,显示“高级 TCP/IP 设置”对话框。
- ③ 打开“WINS”选项卡,如图 4-19 所示。如果需要使用 NetBIOS 名称解析,则选中“启动 LMHOSTS 查询”复选框;如果要使用基于 TCP/IP 协议的 NetBIOS 功能,则选择“启用 TCP/IP 上的 NetBIOS”单选按钮,建议选择这两项。如果该 WINS 客户端从 DHCP 服务器获得 IP 地址,则选择“默认”单选按钮,使用 DHCP 服务器中的 NetBIOS 设置。
- ④ 单击“添加”按钮,显示如图 4-20 所示的“TCP/IP WINS 服务器”对话框,在“WINS 服务器”文本框中键入 WINS 服务器的 IP 地址。

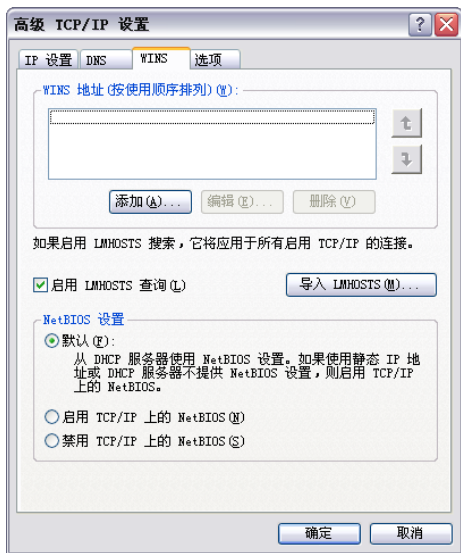


图 4-19 “WINS”选项卡

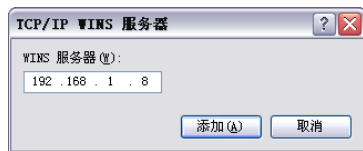


图 4-20 “TCP/IP WINS 服务器”对话框

- ⑤ 单击“添加”按钮,将 WINS 服务器 IP 地址添加到“WINS 地址”列表框中。如果存在多台 WINS 服务器,可按照同样的方法添加。
- ⑥ 依次单击“确定”按钮,保存配置并关闭对话框。

2. Windows Vista 设置

- ① 单击“开始”→“控制面板”→“网络和共享中心”选项,打开“网络和共享中心”窗口。
- ② 在“网络”选项区域中单击“查看状态”超级链接,显示“本地连接 状态”对话框,如图 4-21 所示。
- ③ 单击“属性”按钮,显示“本地连接 属性”对话框,在“此连接使用下列项目”列表框中选择“Internet 协议版本 4 (TCP/IPv4)”选项。单击“属性”按钮,打开“Internet 协议版本 4 (TCP/IPv4) 属性”对话框。
- ④ 单击“高级”按钮,显示“高级 TCP/IP 设置”对话框。打开如图 4-22 所示的“WINS”选项卡,在其中添加 WINS 地址。



图 4-21 “本地连接 状态”对话框

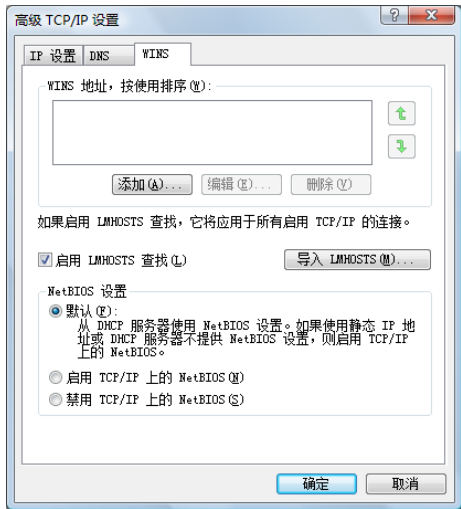


图 4-22 “WINS”选项卡

⑤ 单击“添加”按钮，显示如图 4-23 所示的“TCP/IP WINS 服务器”对话框，在“WINS 服务器”文本框中键入 WINS 服务器的 IP 地址。

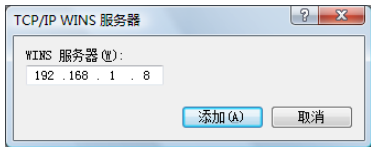


图 4-23 “TCP/IP WINS 服务器”对话框

⑥ 单击“添加”按钮，添加 WINS 服务器址。如果网络中有多台 WINS 服务器，可按相同步骤继续添加。

⑦ 添加完成后，依次单击“确定”按钮保存配置。

4.3.3 在自动获得 IP 地址的客户端上验证

为了验证 DHCP 客户端在获得 IP 地址时是否能够获得 WINS 服务器，可通过运行 ipconfig 命令查看，这里以 Windows Vista 为例。

打开命令提示符窗口，键入“ipconfig /all”命令。按回车键，显示本地连接信息。在“主 WINS 服务器”选项区域中，显示 WINS 服务器的 IP 地址。表示客户端计算机已成功分配 WINS 服务器地址，如图 4-24 所示。

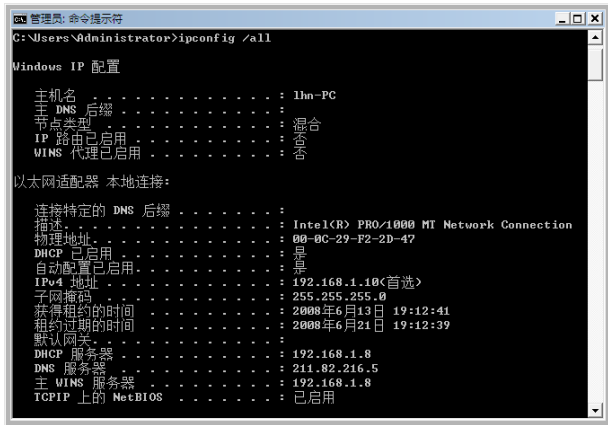


图 4-24 验证 WINS 服务器的 IP 地址

第 5 章 配置与管理 DNS 服务

在网络中，计算机之间都是通过 IP 地址定位并通信的，但是纯数字的 IP 地址非常难记，而且易出错。而利用 DNS（Domain Name System，域名系统）服务可以将 IP 地址与形象易记的域名一一对应，使用户访问主机时不再使用 IP 地址，而是使用域名，DNS 服务器自动解析为 IP 地址并定位服务器。如今大部分发布到 Internet 中的服务器，如 Web、FTP 及 E-mail 等网站都是使用域名。

5.1 DNS 概述

DNS 用于实现名称与 IP 地址转换，它广泛用于局域网、广域网，以及 Internet 等 TCP/IP 网络中。DNS 由名字分布数据库组成，建立了叫做“域名空间”的逻辑树结构。它是负责分配、改写及查询域名的综合性服务系统，其中的每个节点或域都拥有一个唯一的名字。

5.1.1 DNS 系统结构

DNS 系统由 DNS 域名空间、DNS 资源记录、DNS 服务器和 DNS 客户端 4 个部分组成，其主要意义如下。

- (1) DNS 域名空间，指定用于组织名称的域的层次结构。
- (2) DNS 资源记录，将 DNS 域名映射到特定类型的资源信息，以供在命名空间中注册或解析名称时使用。
- (3) DNS 服务器，用于存储和应答资源记录的名称查询。
- (4) DNS 客户端，也称为“解析程序”，用于查询服务器，以搜索并将名称解析为查询中指定的资源记录类型。

1. DNS 域名空间

DNS 域名由主机记录、域名称和顶级域名组成，分别使用英文句点分隔，例如 `www.coolpen.net`。需要说明的是，DNS 解析域名由右向左解释。例如在域名“`www.coolpen.net`”中，“`cn`”表示根服务器，即顶级域；“`coolpen`”是在“`cn`”下注册的域名；“`www`”则是在“`coolpen.net`”的域名中注册的主机记录。如果在“`coolpen.net`”下再注册域名，则可称为“子域”或“二级域名”，如“`bj.coolpen.net`”。每一级域名下都可以注册其他记录。

为了便于为 Internet 提供服务，应使用在 Internet 上有效的域名。一个域名可以通过添加不同的主机来提供不同的服务，例如 Web 服务使用 `www.coolpen.net`，FTP 服务使用 `ftp.coolpen.net`，邮件服务使用 `mail.coolpen.net` 等。

2. DNS 与 Internet

如果需要使用在 Internet 上有效的 DNS 域名，则必须首先向域名服务商（如万网 <http://www.net.cn> 和新网 <http://www.xinnet.com/>）申请合法的域名，并在 DNS 服务器上设置相应的域名解析。不同的顶级域名适用于不同的用途，如表 5-1 所示。

表 5-1 不同顶级域名的用途

顶级域名	用 途
com	供商业组织使用
edu	供教育机构使用
gov	供政府机构使用
mil	供军事机构使用
net	供提供 Internet 或电话服务的组织使用
org	供非商业非营利单位使用
cn	代表中国

顶级域名又可分为国际顶级域名和国家顶级域名，前者指向国际域名管理机构申请并可以在国际上使用的域名类型，如 com、net 及 org 等；后者指在本国内申请使用的域名。大多数国家都按照国家代码分配了不同的顶级域名，例如，我国在国际上的代码为 cn，可以使用的域名有 cn、com.cn、net.net、edu.cn 及 gov.cn 等。

5.1.2 DNS 查询的工作过程与原理

当 DNS 客户端需要访问一个 DNS 域名时，它会查询 DNS 服务器来解析该名称。客户端发送的每条查询消息都包括 3 条信息，作为指定服务器回答的问题。

- (1) 指定的 DNS 域名，规定为完全合格的域名 (FQDN)。
- (2) 指定的查询类型，可根据类型指定资源记录或者查询操作的专用类型。
- (3) DNS 域名的指定类别。

DNS 查询进程分为如下两个部分。

- (1) 名称查询从客户端计算机开始，并传输至解析程序，即 DNS 客户端服务程序进行解析。
- (2) 不能在本地解析查询时可根据需要查询 DNS 服务器来解析名称。

当客户端请求 DNS 查询时，首先会从本地解析程序的缓存查询，通常会从如下两个可能的来源获取名称信息。

(1) 如果在本地配置主机文件，则在 DNS 客户端服务启动时会预先将来自该文件的所有主机名称及地址映射加载到缓存中。

(2) 从以前的 DNS 查询应答的响应中获取的资源记录，将被添加至缓存并保留一段时间。

如果此查询与缓存中的项目不匹配，则解析过程继续进行，由 DNS 服务器来解析名称。当 DNS 服务器接收到查询时，首先检查在本地配置区域的资源记录信息。如果查询的名称与本区域信息中的相应资源记录匹配，则使用该信息来解析查询的名称，服务器做出权威性的应答。

如果区域信息中没有查询的名称，则 DNS 服务器就会检查其本地缓存信息进行解析；如果从中发现匹配的信息，则服务器使用该信息来应答发出请求的客户端，此次查询完成。

如果查询名称没有在本地区域信息发现匹配的应答，则查询进程继续进行，使用递归来完全解析名称。

例如，客户端查询 www.coolpen.net 时，如果在本地缓存信息不能解析该名称，便向 DNS 服务查询，启动查询过程：

首先，DNS 服务器分析并确定顶级域名“net”的位置，DNS 服务器使用迭代查询，以获取“coolpen.net”服务器的信息。然后从“coolpen.net”服务器上查询“www”的主机记录，与服务器 www.coolpen.net 建立联系。最后 www.coolpen.net 服务器将向客户端发出应答，并将客户端查询的信息发送到客户端计算机。

5.1.3 DNS 的反向查找

DNS 的正向查找功能可以将 DNS 域名解析成 IP 地址，而反向查找功能用于让 DNS 客户端通过

IP 地址来查找其主机名称,例如,DNS 客户端可以查找拥有 IP 地址为 211.82.216.5 的主机名称。反向区域并不是必要的,也可在需要时创建。例如,若在 IIS 网站利用主机名称来限制联机的客户端,则 IIS 需要利用反向查找来检查客户端的主机名称。

当利用反向查找来将 IP 地址解析成主机名时,反向区域的前面半部分是其网络 ID (Network ID) 的反向书写,而后半部分必须是.in-addr.arpa。in-addr.arpa 是 DNS 标准中为反向查找定义的特殊域,并保留在 Internet DNS 名称空间中,以便提供切实可靠的方式执行反向查询。例如,如果要针对网络 ID 为 211.82.216.5 的 IP 地址来提供反向查找功能,则此反向区域的名称必须是 5.216.82.211.in-addr.arpa。反向查找采取问答形式进行,就如同向 DNS 服务器询问“您能告诉我使用 IP 地址 211.82.216.5 的计算机的 DNS 域名吗?”。

由于是建立在 DNS 中,所以 in-addr.arpa 域树要求定义其他资源记录 (RR) 类型-指针 (PTR) RR。这种 RR 用于在反向查找区域中创建映射,它一般对应于其正向查找区域中某一主机的 DNS 计算机名的主机 (A) 命名的 RR。

►► 5.1.4 DNS 转发器

转发器也是网络上的 DNS 服务器,用来将外部 DNS 名称的 DNS 查询转发给外网的 DNS 服务器。

一般情况下,当 DNS 服务器在收到 DNS 客户端的查询请求后,它将在所管辖区域的数据库中查找是否有该客户端的数据。如果没有(即在 DNS 服务器所管辖的区域数据库中该 DNS 客户端所查询的主机名),则该 DNS 服务器需转向其他 DNS 服务器进行查询。

在实际应用中,以上这种现象经常发生。例如,当网络中的某台主机要与位于本网络外的主机通信时就需要向外界的 DNS 服务器进行查询,并由其提供相应的数据。但为了安全起见,一般不希望内部所有的 DNS 服务器都直接与外界 DNS 服务器建立联系。而是只让一台 DNS 服务器与外界建立直接联系,网络内的其他 DNS 服务器则通过这一台 DNS 服务器来与外界间接联系,将这台直接与外界建立联系的 DNS 服务器称之为“转发器”。

有了转发器后,当 DNS 客户端提出查询请求时,DNS 服务器将通过转发器从外界 DNS 服务器中获得数据,并将其提供给 DNS 客户端。如果转发器无法查询到所需的数据,则 DNS 服务器一般提供如下两种处理方式。

(1) DNS 服务器直接向外界的 DNS 服务器进行查询。

(2) DNS 服务器不再向外界的 DNS 服务器进行查询,而是告诉 DNS 客户端找不到所需的数据。

如果是后一种方式,该 DNS 服务器将完全依赖于转发器。出于安全上的考虑,最好将 DNS 服务器设置为这种方式。即完全依赖于转发器的方式,这样的 DNS 服务器就叫做“从属服务器”。

►► 5.1.5 动态更新

动态更新允许 DNS 客户端在发生更改时,使用 DNS 服务器注册并动态地更新其资源记录,从而减少了手工管理的麻烦。对于频繁移动或改变位置的 DHCP 客户端,应启用动态更新功能,以便于及时更新地址。

DNS 客户端和服务端支持使用动态更新,DNS 服务器服务允许在配置为加载标准主要区域或目录集成区域的每个服务器上的每个区域上启用或禁用动态更新。默认情况下,DNS 客户端服务在配置用于 TCP/IP 时,将动态更新 DNS 中的主机资源记录。

默认情况下,静态配置用于 TCP/IP 的计算机尝试为其安装的网络连接所配置和使用的 IP 地址动态注册主机 (A) 和指针 (PTR) 资源记录 (RR)。默认情况下,所有计算机都基于其完全限定的域名 (FQDN) 注册记录。

►► 5.1.6 活动目录集成

从 Windows 2000 Server 开始, DNS 服务器服务已集成到 Active Directory 的设计和实施中。在服务器上安装 Active Directory 时, 可以将服务器升级为指定域的域控制器角色。完成该过程时, 系统将提示为要加入和升级服务器的 Active Directory 域指定 DNS 域名。

如果在该过程中, 在网络上找不到指定域的权威 DNS 服务器, 或不支持 DNS 动态更新协议, 系统将提示通过相关选项安装 DNS 服务器。之所以提供该选项, 原因在于定位该服务器或作为 Active Directory 域成员的其他域控制器时需要 DNS 服务器。

安装 Active Directory 之后, 操作新的域控制器上运行的 DNS 服务器时, 可以使用两种存储和复制区域的选项。

(1) 使用基于文本文件的标准区域存储: 按这种方式存储的区域位于 .Dns 文件中, 这些文件存储在运行 DNS 服务器的每台计算机上的 systemroot\System32\Dns 文件夹中。区域文件名称与创建区域时为区域选择的名称相对应, 例如区域名称为 coolpen.net, 则区域文件为 coolpen.net.dns。

(2) 使用 Active Directory 数据库的目录集成区域存储: 按这种方式存储的区域位于域或应用程序目录分区下的 Active Directory 树中, 每个目录集成区域都存储在按照创建该区域时为其选择的名称标识的 DNS Zone 容器对象中。

5.2 安装 DNS 服务器

DNS 服务默认没有安装在 Windows Server 系统中, 需要网络管理员手动添加。在 DNS 服务之前, 应首先准备已向域名申请机构申请的正式域名, 同时 DNS 服务器还必须拥有固定并可被 Internet 访问的 IP 地址。

►► 5.2.1 安装活动目录的 DNS 要求

Active Directory 将 DNS 作为域控制器的定位机制, 使网络上的计算机可以获取域控制器的 IP 地址。在安装 Active Directory 时, 会向 DNS 动态注册服务 (SRV) 和地址 (A) 资源记录, 这些记录是域控制器定位程序功能成功实现所必需的。

要在域或林中查找域控制器, 客户端将在 DNS 中查询域控制器的 SRV 和地址 DNS 资源记录, 这些资源记录为客户端提供域控制器的名称和 IP 地址。在这种环境中, SRV 和 A 资源记录被称为“定位程序 DNS 资源记录”。

在林中添加域控制器时, 将使用定位程序 DNS 资源记录更新 DNS 服务器上主持的 DNS 区域, 同时标识域控制器。为此, DNS 区域必须允许动态更新, 同时主持该区域的 DNS 服务器必须支持 SRV 资源记录才能公布 Active Directory 目录服务。如果主持权威 DNS 区域的 DNS 服务器不是运行 Windows Server 2000/2003/2008 系统的服务器, 则要与 DNS 管理员联系, 确定该 DNS 服务器是否支持所需的标准。如果服务器不支持所需标准, 或者权威 DNS 区域不能被配置为允许动态更新, 则需要修改现有 DNS 结构。

►► 5.2.2 安装 DNS 服务

安装 DNS 服务的操作步骤如下。

① 以管理员账户登录到 Windows Server 2008 系统, 运行“添加角色向导”, 在如图 5-1 所示的“选择服务器角色”对话框中的“角色”列表框中选中“DNS 服务器”复选框。

② 单击“下一步”按钮, 显示如图 5-2 所示的“DNS 服务器”对话框, 其中显示 DNS 服务器的概述信息。

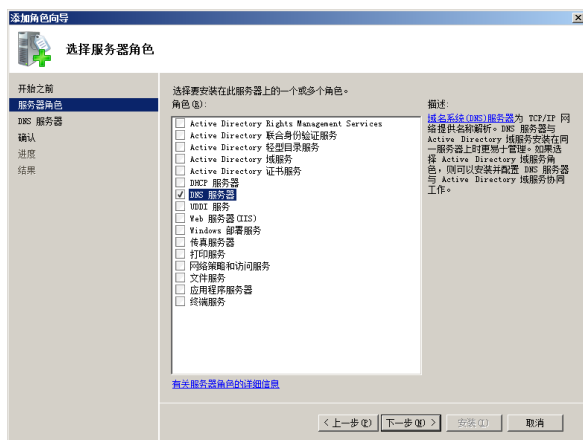


图 5-1 “选择服务器角色”对话框



图 5-2 “DNS 服务器”对话框

③ 单击“下一步”按钮，显示如图 5-3 所示的“确认安装选择”对话框，要求确认所要安装的角色。

④ 单击“安装”按钮，开始安装 DNS 服务。完成后显示如图 5-4 所示的“安装结果”对话框，提示 DNS 服务器已经安装成功。

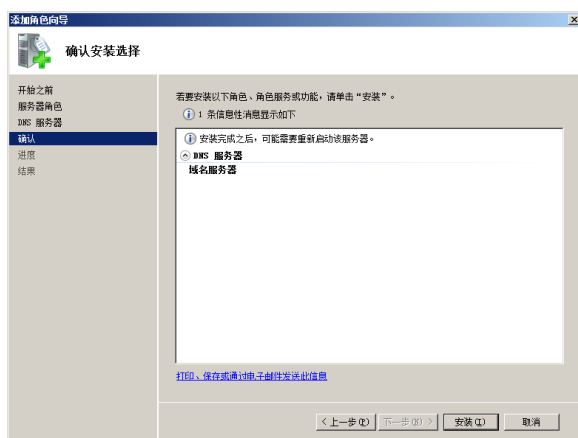


图 5-3 “确认安装选择”对话框

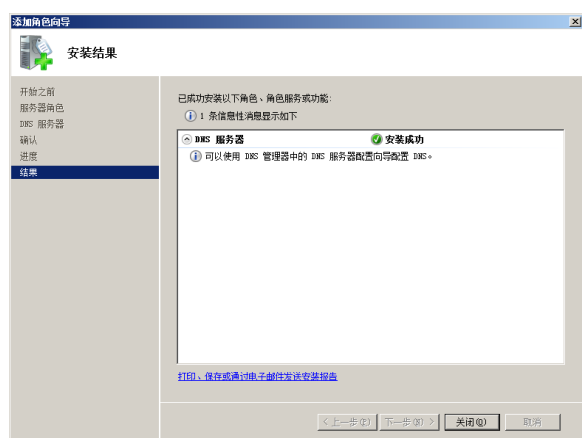


图 5-4 “安装结果”对话框

⑤ 单击“关闭”按钮，返回“初始配置任务”窗口。单击“开始”→“管理工具”→“DNS”选项，显示“DNS 管理器”窗口，如图 5-5 所示，在其中可配置 DNS 服务。

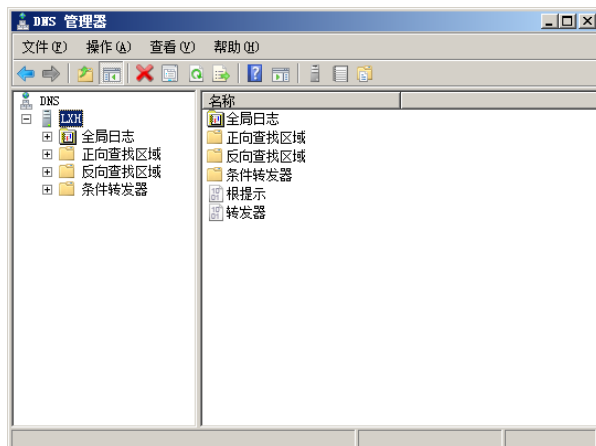


图 5-5 “DNS 管理器”窗口

**提示**

与 Windows Server 2003 不同, Windows Server 2008 在安装 DNS 服务时并不会出现 DNS 配置向导, 需要在安装完成后配置。

5.3 配置与管理 DNS 服务器

在安装 DNS 服务时, 由于不会启动配置向导, 因此需要在安装完成以后配置 DNS 域。添加相应的正、反向查找区域及各种主机记录, 将域名与相应的 IP 地址一一关联起来。从而为网络提供解析服务, 使用户能够通过域名来访问网络中的主机。

5.3.1 添加正向搜索区域

为了使 DNS 服务器能够将域名解析成 IP 地址, 必须首先在 DNS 区域中添加正向查找区域。并且可以添加多个区域, 以解析多个域名。

① 打开“DNS 管理器”窗口, 展开左侧目录树。选择“正向查找区域”选项, 显示尚未添加的区域, 如图 5-6 所示。

② 右击“正向查找区域”选项, 选择快捷菜单中的“新建区域”选项。显示“新建区域向导”对话框, 如图 5-7 所示。

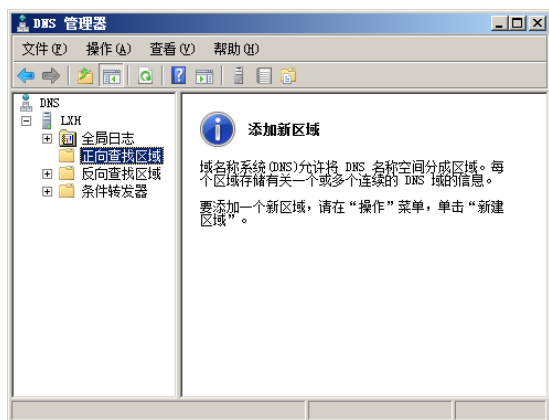


图 5-6 尚未添加的区域

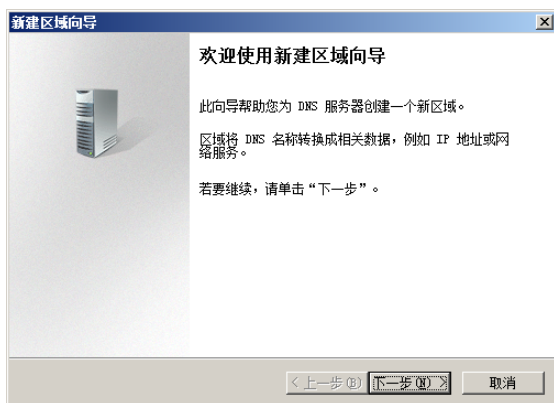


图 5-7 “新建区域向导”对话框

③ 单击“下一步”按钮, 显示如图 5-8 所示的“区域类型”对话框, 在其中选择要创建的区域类型。如果要直接在当前服务器创建 DNS 区域, 则选择“主要区域”单选按钮; 如果要在其他服务器上创建, 则选择“辅助区域”单选按钮; 如果创建只含有名称服务器 (NS)、起始授权机构 (SOA) 和粘连主机 (A) 记录的区域, 则选择“存根区域”单选按钮。

④ 单击“下一步”按钮, 显示如图 5-9 所示的“区域名称”对话框。在“区域名称”文本框中键入在域名服务机构申请的正式域名, 如“coolpen.net”。区域名称用于指定 DNS 名称空间的部分, 可以是域名或者子域名 (hs.coolpen.net)。

⑤ 单击“下一步”按钮, 显示如图 5-10 所示的“区域文件”对话框。选择“创建新文件, 文件名为”单选按钮, 创建一个新的区域文件, 文件名使用默认即可。如果要从另一个 DNS 服务器将记录文件复制到本地计算机, 则选中“使用此现存文件”单选按钮并输入现存文件的路径。

⑥ 单击“下一步”按钮, 显示如图 5-11 所示的“动态更新”对话框, 在其中选择如下动态更新方式。

只允许安全的动态更新 (适合 Active Directory 使用): 只有在安装了 Active Directory 的区域才能选择该选项。

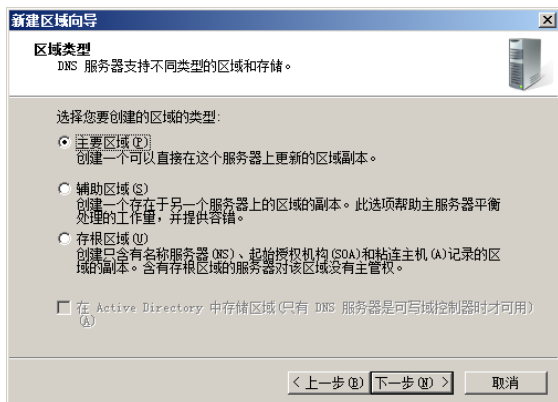


图 5-8 “区域类型”对话框

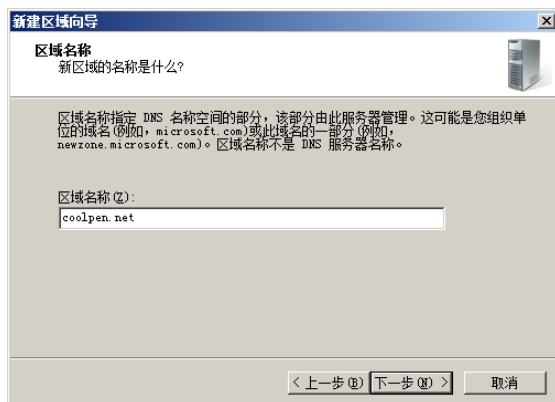


图 5-9 “区域名称”对话框

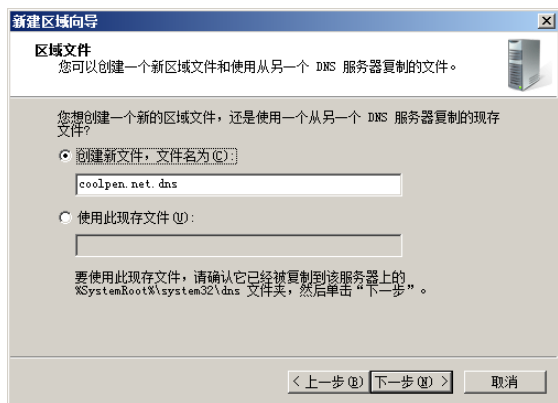


图 5-10 “区域文件”对话框

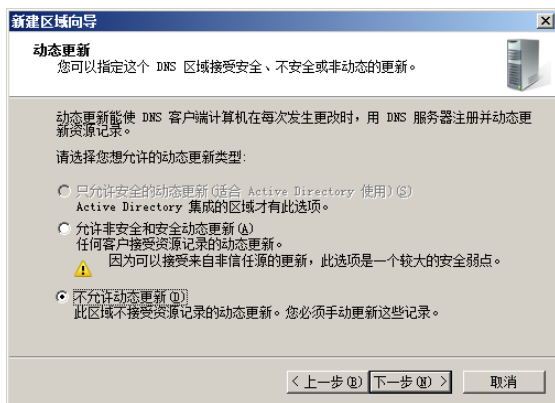


图 5-11 “动态更新”对话框

允许非安全和安全动态更新：选择该选项，使任何客户端都可接受资源记录的动态更新。由于也可接受来自非信任源的更新，所以可能会不安全。

不允许动态更新：可使此区域不接受资源记录的动态更新，使用此选项比较安全。

⑦ 单击“下一步”按钮，显示如图 5-12 所示的“正在完成新建区域向导”对话框，显示前面所做的设置。

⑧ 单击“完成”按钮完成向导，创建完成“coolpen.net”区域，如图 5-13 所示。

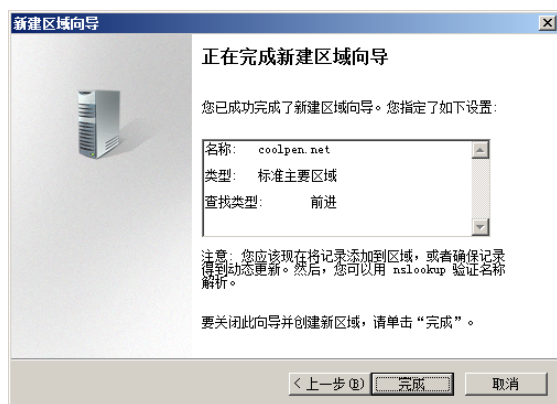


图 5-12 “正在完成新建区域向导”对话框

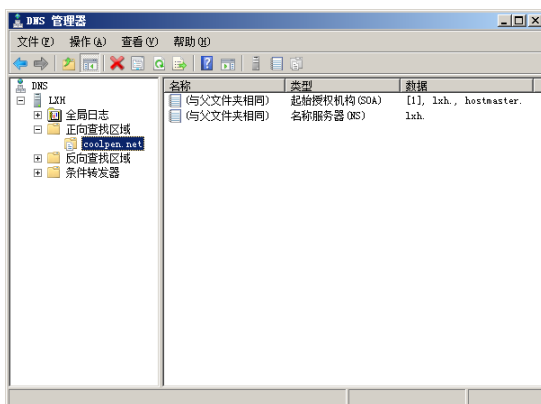


图 5-13 创建完成“coolpen.net”区域

重复上述操作过程，可以添加多个 DNS 区域。并且分别指定不同的域名称，从而为多个 DNS 域名提供解析。

5.3.2 添加 DNS 区域

DNS 区域 (Zone) 是 DNS 服务最基本的管理控制单元, 在一台 DNS 服务器上可以创建多个区域。如果网络规模比较大, 并且用户数量比较多时, 则可以在区域内划分多个子区域, 以方便管理。例如, 在企业为网络管理中销售部拥有自己的服务器。但是为了方便管理, 还可以为不同地区的销售分部设置单独的子域, 在这个域中添加主机记录及其他资源记录 (如别名记录等)。另外, 大中型高校校园网络也是如此。

① 选择要划分子域的 DNS 区域, 如 coolpen.net。右击并选择快捷菜单中的“新建域”选项, 显示如图 5-14 所示的“新建 DNS 域”对话框。输入待划分的子域名称, 如 hbhs。

② 单击“确定”按钮, 创建完成新子域, 如图 5-15 所示。

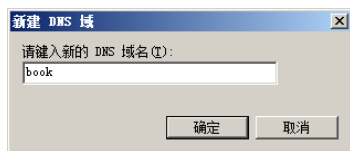


图 5-14 “新建 DNS 域”对话框

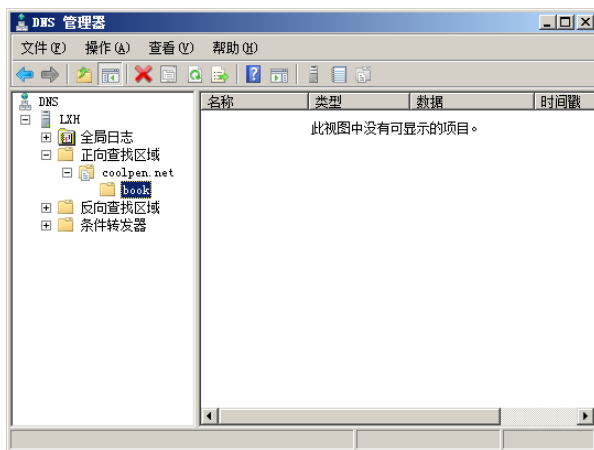


图 5-15 创建完成新子域

此时就可以在 DNS 子域中添加主机记录及继续创建子域等, 操作方法与该机 DNS 区域类似。需要注意的是, 如果删除某个域或子域, 则其包含的下属子域也将同时被删除。

5.3.3 添加 DNS 记录

DNS 服务器配置完成以后, 要为所属的域 (如 coolpen.net) 提供域名解析服务, 还必须在 DNS 域中添加各种 DNS 记录, 如 Web 及 FTP 等使用 DNS 域名的网站等都需要添加 DNS 记录来实现域名解析。

1. 添加主机记录 (A)

主机记录的作用是将主机的相关参数 (主机名和对应的 IP 地址) 添加到 DNS 服务器中, 这样 DNS 客户端就可以通过查询主机名或 IP 地址来访问相应的站点。Web 及 FTP 等服务器的域名就是一个主机记录, 类似于 www.sohu.com 及 ftp.china.com 等。

① 在 DNS 控制台中选择要创建主机记录的区域, 如 coolpen.net。右击并选择快捷菜单中的“新建主机”选项, 显示如图 5-16 所示的“新建主机”对话框。在“名称”文本框中键入主机名称, 如 www, 同时在“完全合格的域名”中显示完整的名称, 在“IP 地址”文本框中键入主机对应的 IP 地址。

② 单击“添加主机”按钮, 显示如图 5-17 所示的提示框, 提示主机记录创建成功。

③ 单击“确定”按钮, 创建完成主机记录 www.coolpen.net, 如图 5-18 所示。当用户访问该地址时, DNS 服务器即可自动解析成相应的 IP 地址。按照同样步骤, 可以添加多个主机记录。

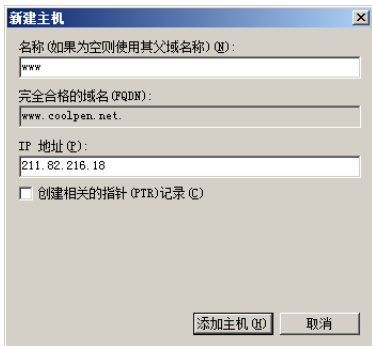


图 5-16 “新建主机”对话框



图 5-17 提示框

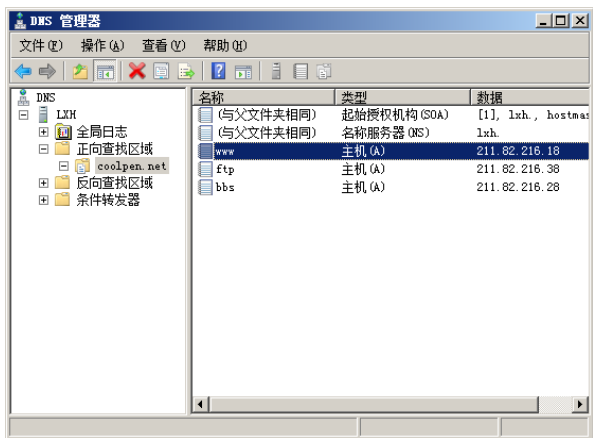


图 5-18 主机记录 www.coolpen.net

2. 添加邮件交换器记录（MX）

邮件交换器（MX）资源记录为电子邮件服务专用，用来表示所属邮件服务器的 IP 地址。用户在使用邮件程序发送邮件时，根据收信人地址后缀向 DNS 服务器查询邮件交换器资源记录，从而定位到接收邮件服务器。例如，在 DNS 区域“coolpen.net”中有一个邮件服务器。向用户的邮箱 liuxh@coolpen.net 发送邮件时，系统就会检查邮件地址中的域名 coolpen.net 的 MX 记录，并将邮件转发到相应的邮件服务器上。

① 在“DNS 管理器”窗口中选择 DNS 区域（coolpen.net），右击并在快捷菜单中选择“新建邮件交换器（MX）”选项，显示如图 5-19 所示的“新建资源记录”对话框。

在其中设置如下选项。

主机或子域：输入此邮件交换器（一般是指邮件服务器）记录的域名，如果要创建类似@coolpen.net 的邮件服务器的 MX 记录，则此处保留为空。

邮件服务器的完全合格的域名：设置域中负责邮件发送或接收的邮件服务器的全称域名 FQDN（如 pop.coolpen.net），或单击“浏览”按钮选择。

邮件服务器优先级：当该区域内有多台邮件服务器时，可以设置其优先级。数值越小，则优先级越高（0 最高）。范围为 0~65535，优先级高的邮件服务器会被优先选择。如果有两台以上的邮件服务器的优先级相同，则系统会随机选择。

提示



大型邮件系统中的 SMTP 服务器和 POP3 服务器通常不在同一台服务器上，因此需要分别使用 smtp 和 pop（或 pop3）的主机记录；中小型系统中的 SMTP 服务器和 POP3 服务器通常位于同一台服务器，一般只创建一条主机记录即可，并且使 MX 记录指向该记录。当然也可以创建名为“pop”、“pop3”及“smtp”的主机记录，以满足大多数人的习惯。

- ② 单击“确定”按钮，邮件交换器记录添加成功。

3. 添加别名记录

别名记录用于将 DNS 域名的别名映射到另一个主要或规范的名称。有时一台主机可能担当多个服务器，因此需要为该主机创建多个别名。例如，一台主机既是 Web 服务器，也是 FTP 服务器，这时就要为其创建多个别名。

① 在 DNS 控制台中选择 DNS 区域，右击并选择快捷菜单中的“新建别名”选项，显示如图 5-20 所示的“新建资源记录”对话框。在“别名”文本框中键入主机别名，在“目标主机的完全合格的域名”文本框中键入指派该别名的主机名称，如 www.coolpen.net。

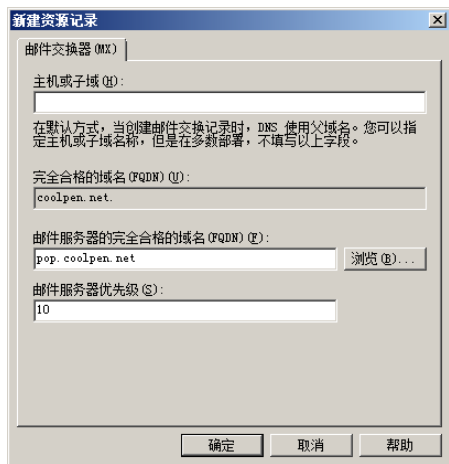


图 5-19 “新建资源记录”对话框

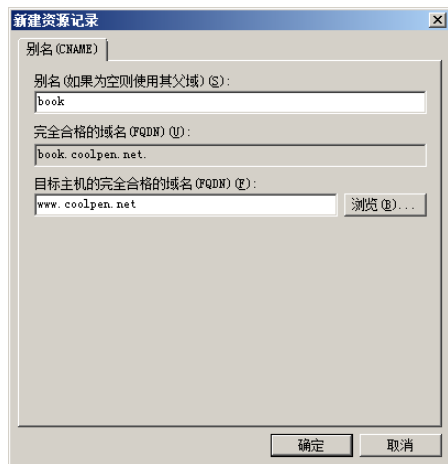


图 5-20 “新建资源记录”对话框

- ② 单击“确定”按钮，别名添加完成。



注意：

“别名”必须是主机名，而不能是全称域名 FQDN；而“目标主机的完全合格的域名”文本框中的名称必须是全称域名 FQDN，不能是主机名。



5.3.4 添加反向查找区域

反向查找区域和正向查找区域正好相反，其功能是将 IP 地址解析成 DNS 域名。在网络中，大部分 DNS 搜索都是正向查找。但为了实现客户端对服务器的访问，不仅需要将一个域名解析成 IP 地址，还需要将 IP 地址解析成域名，这就需要使用反向查找功能。在 DNS 服务器中，通过主机名查询其 IP 地址的过程称为“正向查询”，而通过 IP 地址查询其主机名的过程称为“反向查询”。

1. 创建反向查找区域

① 打开“DNS 管理器”窗口，选择“反向查找区域”选项。右击并选择快捷菜单中的“新建区域”选项，打开“新建区域向导”对话框，如图 5-21 所示。

② 单击“下一步”按钮，显示如图 5-22 所示的“区域类型”对话框，选择“主要区域”单选按钮。

③ 单击“下一步”按钮，显示如图 5-23 所示的“反向查找区域名称”对话框。由于网络中主要使用 IPv4，因此选择“IPv4 反向查找区域”单选按钮。

④ 单击“下一步”按钮，显示如图 4-24 所示的“反向查找区域名称”对话框。在“网络 ID”文本框中输入 IP 地址 211.82.216，同时在“反向查找名称”文本框中显示为 216.82.211.in-addr.arpa。

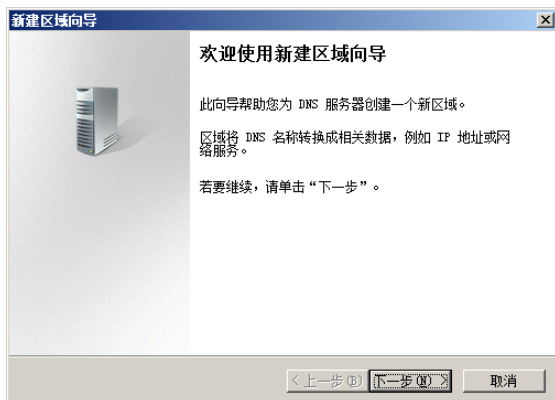


图 5-21 “新建区域向导”对话框

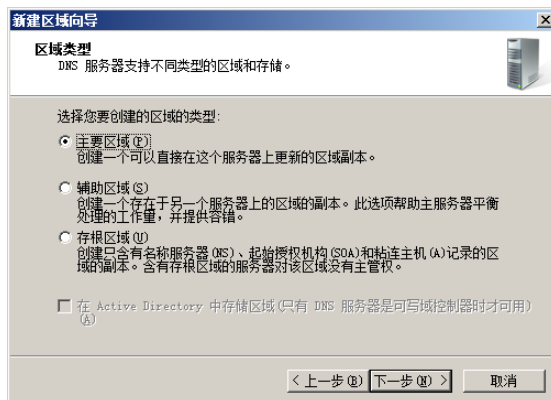


图 5-22 “区域类型”对话框

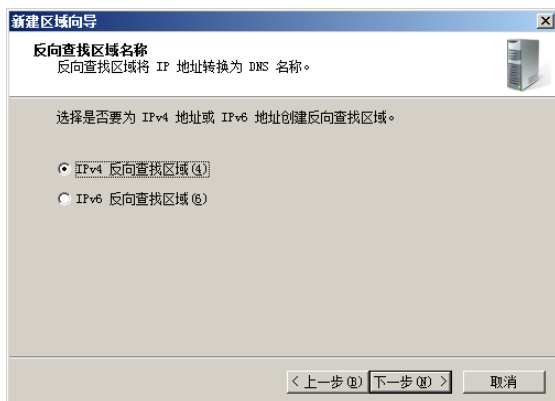


图 5-23 “反向查找区域名称”对话框

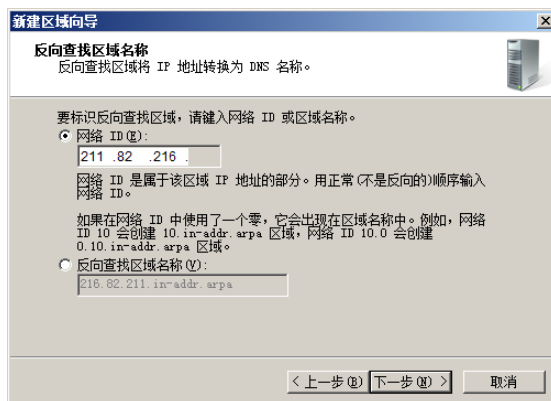


图 5-24 “反向查找区域名称”对话框

⑤ 单击“下一步”按钮，显示如图 5-25 所示的“区域文件”对话框，默认创建一个名为“216.82.211.in-addr.arpa.dns”的区域文件。

⑥ 单击“下一步”按钮，显示如图 5-26 所示的“动态更新”对话框，在其中选择是否要指定这个区域接受安全、不安全或非动态的更新。为了维护 DNS 服务器的安全性，建议选择“不允许动态更新”单选按钮，以减少来自网络的攻击。

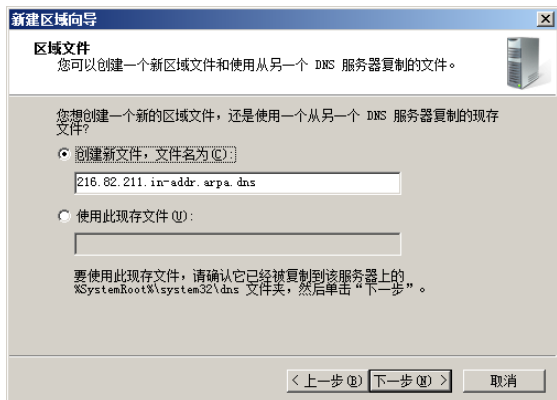


图 5-25 “区域文件”对话框

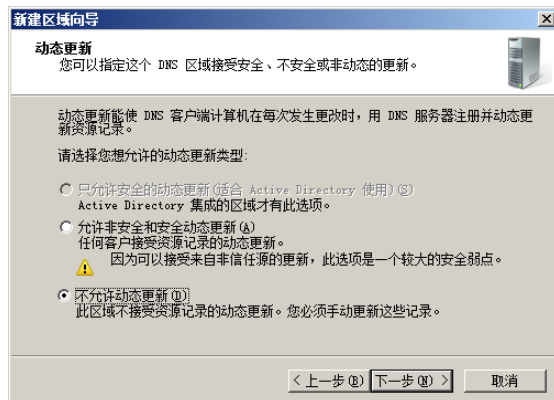


图 5-26 “动态更新”对话框

⑦ 单击“下一步”按钮，显示如图 5-27 所示的“正在完成新建区域向导”对话框，其中列出前面所做的配置信息。

⑧ 单击“完成”按钮，创建完成反向区域，并显示在“DNS 管理器”窗口的“反向查找区域”中。区域名称显示为“216.82.211.in-addr.arpa”，如图 5-28 所示。

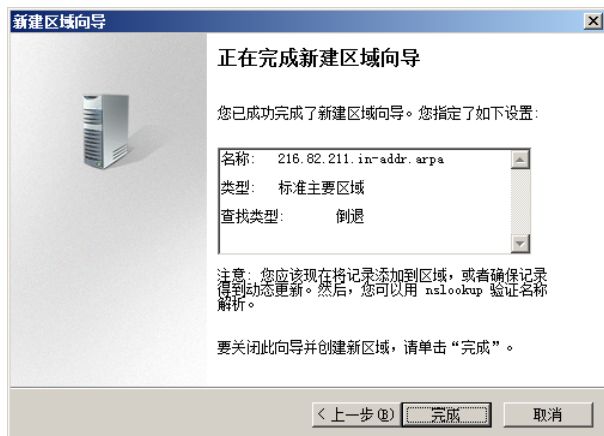


图 5-27 “正在完成新建区域向导”对话框

2. 创建反向记录

当创建完成反向查找区域以后，还必须在其中创建记录数据，使服务器能够通过 IP 地址解析相应的 DNS 域名。

(1) 右击新创建的反向查找区域，选择快捷菜单中的“新建指针”选项，显示如图 5-29 所示的“新建资源记录”对话框。在“主机 IP 地址”文本框中键入主机 IP 地址，在“主机名”文本框中键入该 IP 地址对应的主机名，或单击“浏览”按钮选择。

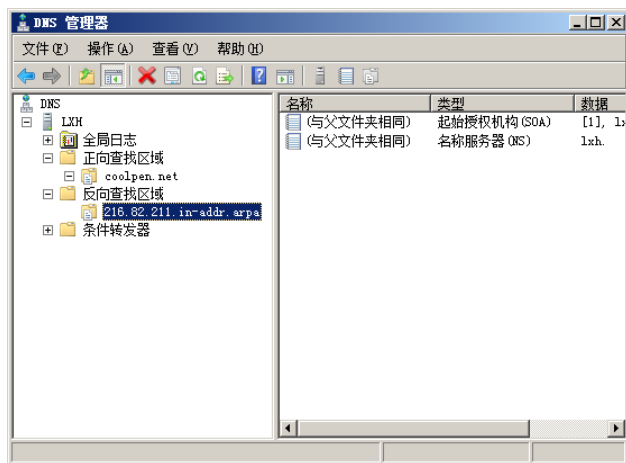


图 5-28 已创建的区域

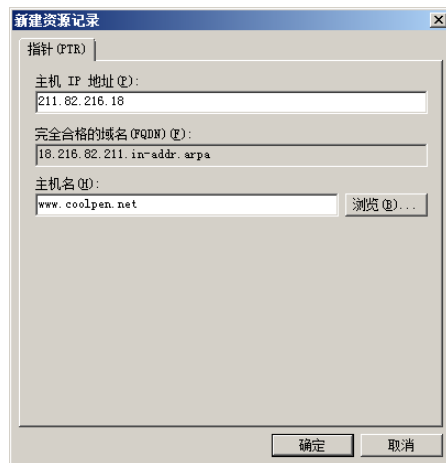


图 5-29 “新建资源记录”对话框

(2) 单击“确定”按钮，创建成功指针记录，按照同样步骤可以添加多个指针记录。

5.3.5 设置转发器

当客户端计算机访问本地网络中的服务器时，可以通过本地网络中的 DNS 服务器解析域名；而当访问 Internet 中的服务器时，本地 DNS 服务器无法提供所需要的数据，为此需要设置一台有转发器功能的 DNS 服务器。将此查询转发到其他 DNS 服务器递归查询，从而为用户解析出相应的 IP 地址。

(1) 在“DNS 管理器”窗口中右击服务器名并选择快捷菜单中的“属性”选项，显示服务器属性对话框。打开“转发器”选项卡，如 5-30 所示。

(2) 单击“编辑”按钮，显示如图 5-31 所示的“编辑转发器”对话框。在“<单击此处添加 IP 地址或 DNS 名称>”文本框中键入转发器的 IP 地址或 DNS 域名，按回车键添加，系统会自动对该转发

器地址进行验证。

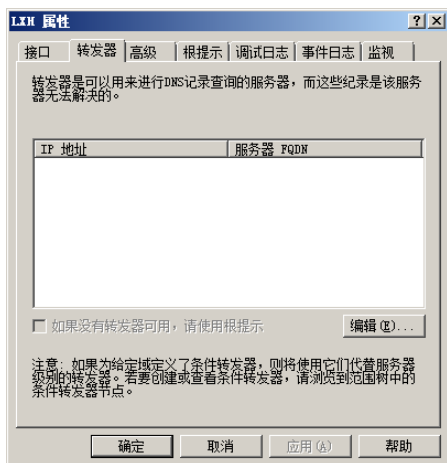


图 5-30 “转发器”选项卡

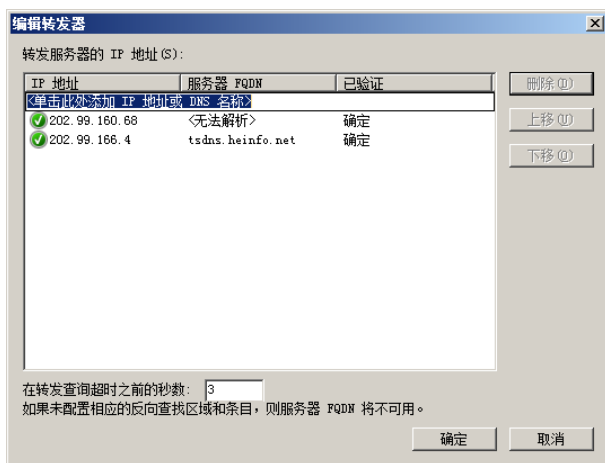


图 5-31 “编辑转发器”对话框

(3) 如果输入的转发器地址无误，能够通过验证，则单击“确定”按钮。添加成功，如图 5-32 所示。

(4) 单击“确定”按钮，DNS 转发器设置成功，网络中的 DNS 客户端即可利用转发器解析 Internet 中的域名。

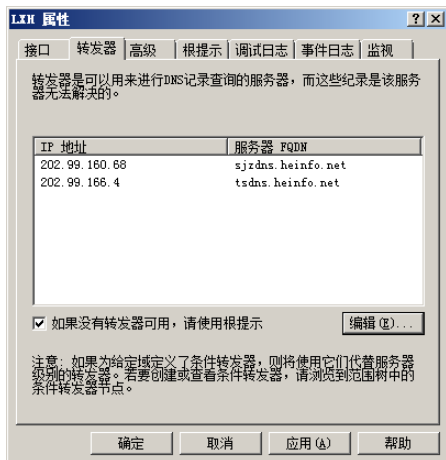


图 5-32 转发器添加成功

5.3.6 添加辅助 DNS 服务器

为了避免由于 DNS 服务器故障导致 DNS 解析失败，通常可安装两台 DNS 服务器，一台作为主服务器；一台作为辅助服务器。当主 DNS 服务器正常运行时，辅助服务器只起备份作用，自动从主 DNS 服务器上获取 DNS 数据。一旦主 DNS 服务器发生故障，辅助 DNS 服务器便立即承担起 DNS 解析服务，代替主 DNS 服务器的地位。

1. 配置主 DNS 服务器

在设置 DNS 辅助服务器之前，应当首先在主 DNS 服务器上添加允许传送的辅助 DNS 服务器地址。并设置“通知”，使主 DNS 服务器上的能够自动通知辅助 DNS 服务器。操作步骤如下。

① 登录到主 DNS 服务器，在 DNS 控制台中打开待设置的 DNS 区域的属性对话框。打开“允许区域传送”选项卡，如图 5-33 所示。选中“允许区域复制”复选框，并选择“只允许到下列服务器”单选按钮。

② 单击“编辑”按钮，显示如图 5-34 所示的“允许区域传送”对话框。在“允许区域传送”对话框中键入辅助 DNS 服务器的 IP 地址或计算机名，按回车键。如果连接成功，则解析出相应的计算机名。

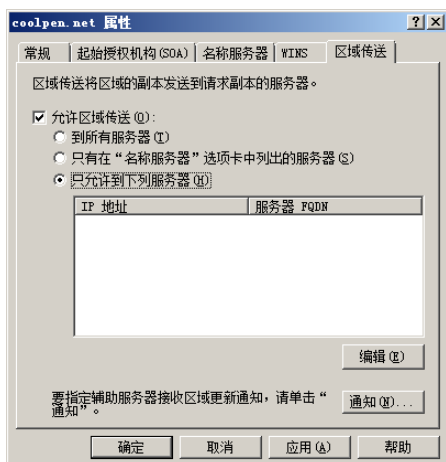


图 5-33 “允许区域传送”选项卡

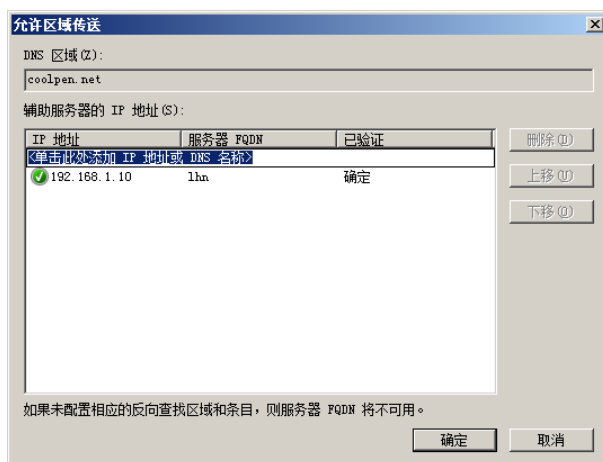


图 5-34 “允许区域传送”对话框

③ 单击“确定”按钮，返回“区域传送”选项卡。单击“通知”按钮，显示如图 5-35 所示的“通知”对话框，选中“自动通知”复选框，选择“下列服务器”单选按钮，在“<单击此处添加 IP 地址或 DNS 名称>”文本框中键入辅助 DNS 服务器的计算机名或 IP 地址，按回车键验证。

④ 依次单击“确定”按钮关闭对话框。

2. 安装辅助 DNS 服务器

登录到辅助 DNS 服务器，执行如下操作安装辅助 DNS 服务器。

① 在辅助 DNS 服务器上安装 DNS 服务。

② 打开“DNS 管理器”窗口，右击“正向搜索区域”选项。选择快捷菜单中的“新建区域”选项，打开“新建区域向导”对话框。

③ 单击“下一步”按钮，显示如图 5-36 所示的“区域类型”对话框。选择“辅助区域”单选按钮，将该计算机设置为辅 DNS 服务器。

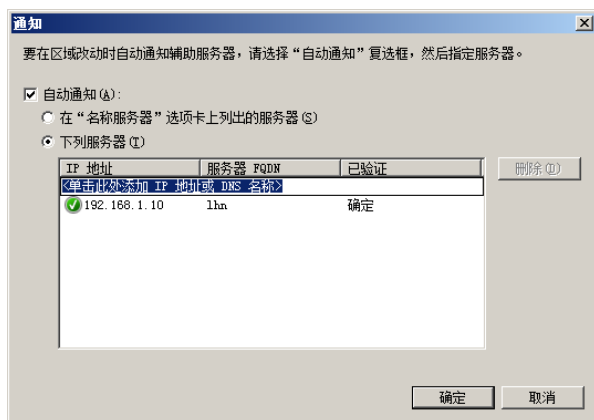


图 5-35 “通知”对话框

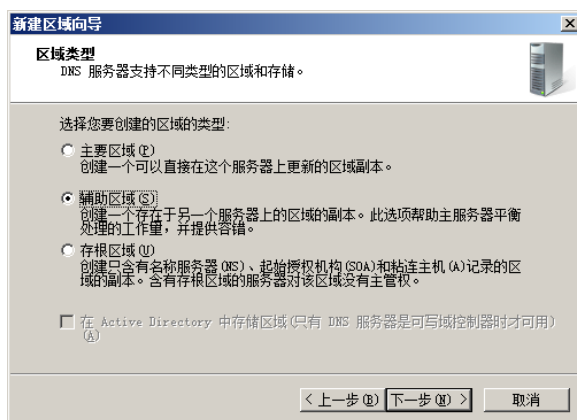


图 5-36 “区域类型”对话框

④ 单击“下一步”按钮，显示如图 5-37 所示的“区域名称”对话框。在“区域名称”文本框中键入创建辅助区域的域名，该名称应与主 DNS 服务器上的 DNS 域名相同。

⑤ 单击“下一步”按钮，显示如图 5-38 所示的“主 DNS 服务器”对话框。在“IP 地址”列表框中键入主 DNS 服务器的 IP 地址，按回车键验证。

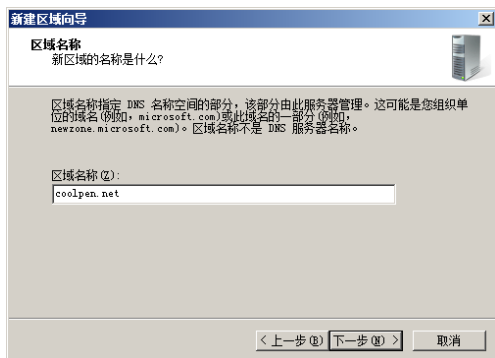


图 5-37 “区域名称”对话框

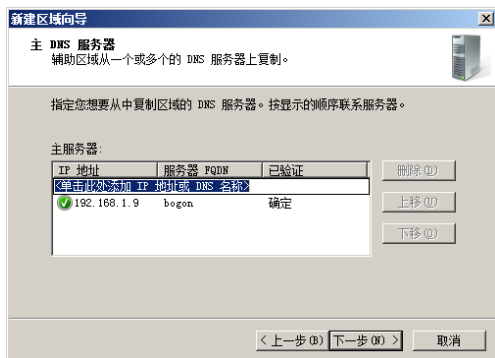


图 5-38 “主 DNS 服务器”对话框

⑥ 单击“下一步”按钮，显示“正在完成新建区域向导”对话框。单击“确定”按钮，辅助区域创建完成。在辅助 DNS 服务器中显示从主 DNS 服务器加域的各种记录信息，如图 5-39 所示。



提示

如果因网络原因，辅助服务器上没有显示主 DNS 服务器上的信息，则右击域名并选择快捷菜单中的“从主服务器重新加载”选项，重新加载并按 F5 键刷新。

创建完成辅助 DNS 服务器以后，将每隔 15 分钟从其主 DNS 服务器执行一次“区域转送”操作，以最大限度地保持辅助服务器中的数据与主 DNS 服务器一致。

5.3.7 备份 DNS 服务器信息

为了避免 DNS 服务器出现故障导致 DNS 数据丢失，应将 DNS 数据备份到其他磁盘或网络驱动器上。当修复 DNS 服务器故障或者将 DNS 服务器迁移到其他服务器上时，只需将备份的数据复制到相应的目录下，即可恢复 DNS 服务器。

DNS 服务器默认会在 %Systemroot%\System32\DNS 目录下创建数据库文件，其中 backup 文件夹用来备份 DHCP 数据库，如图 5-40 所示。

如果备份 DNS 服务器的数据，只需备份 backup 文件夹及其所有文件。当需要还原时，只需将备份的 backup 文件夹中的文件复制到原来的位置即可。



注意

为了保证所备份数据的完整，在备份时应首先在 DNS 控制台中右击服务器名称。选择快捷菜单中的“所有任务”→“停止”选项，以停止 DNS 服务器。

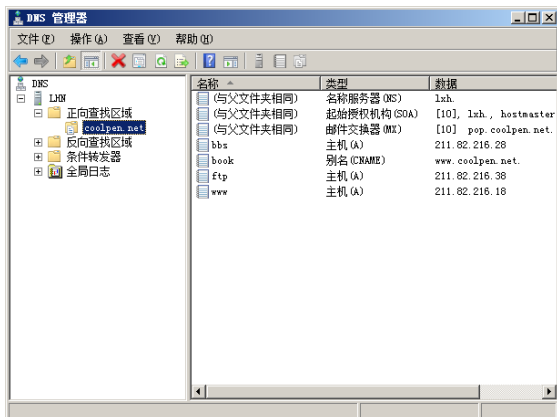


图 5-39 从主 DNS 服务器加域的各种记录信息

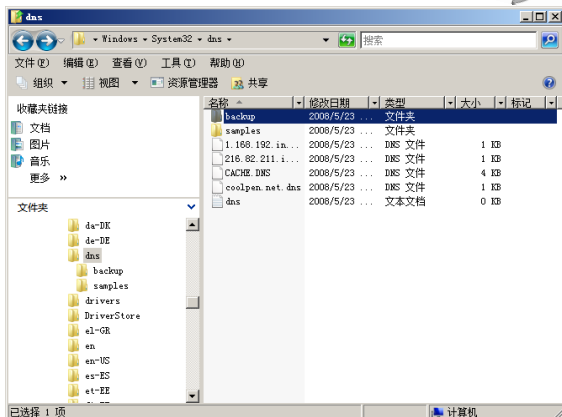


图 5-40 backup 文件夹

第 6 章 配置与管理 DHCP 服务

在 TCP/IP 网络中每台计算机必须分配至少一个 IP 地址，以实现彼此之间的通信。在计算机数量较少的网络中，可以以手动方式设置 IP 地址。但当计算机数量较多时，采用手动方式不仅非常费时、费力，而且也非常容易出错，尤其在大中型网络中这更是一项非常复杂的工作。如果通过 DHCP (Dynamic Host Configuration Protocol, 动态主机分配协议) 服务使得服务器自动为客户端计算机配置 IP 地址信息，就可以大大提高工作效率，并减少发生 IP 地址故障发生的可能性。

6.1 DHCP 服务概述

DHCP 是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议，网络管理员可以利用 DHCP 服务器动态地为客户端分配 IP 地址及其他相关的环境配置工作。

6.1.1 DHCP 服务简介

计算机配置 IP 地址的方式有两种，一是手动键入的静态 IP 地址；二是使用 DHCP 服务器分配的动态 IP 地址。采用手动分配静态 IP 地址，如果只有几台计算机，则设置比较简单。但是当网络比较大，有几十台，甚至几百台计算机时，就容易出现错误。不仅效率低下，而且劳动强度大；采用动态 IP 地址，由于 IP 地址是 DHCP 服务器自动分配，客户端计算机自动获取。从而有效地避免了可能出现的键入错误，大大减轻了劳动强度。并且提高了工作效率，因此 DHCP 服务非常适合大中型网络。

DHCP 是一种非常优秀的 IP 地址管理工具，主要具有以下优点。

(1) 提高效率

网络中的计算机将自动从 DHCP 服务器获得 IP 地址信息并进行配置，不需人工干预。从而极大地提高工作效率，降低了劳动强度。并可以避免键入错误，减少了许多可能由 TCP/IP 设置问题而导致的网络故障。

(2) 便于管理

当网络使用的 IP 地址段改变时，只需修改 DHCP 服务器的 IP 地址池即可，不必逐台修改网络内的所有计算机。

(3) 节约 IP 地址资源

利用 DHCP 服务时，只有当 DHCP 客户端请求时才由 DHCP 服务器提供 IP 地址。当计算机关机后，又会自动释放该 IP 地址。通常情况下，网络内的计算机并不都是同时开机。因此即使 IP 地址数量较少，也能够满足较多计算机的需求。

当然，DHCP 也存在一些缺点。如果 DHCP 服务器设置有误或出现故障，将会影响网络中所有 DHCP 客户端无法正常获得 IP 地址。另外，如果网络中只有一台 DHCP 服务器，当其故障时，所有 DHCP 客户端都将既无法获得 IP 地址，也无法释放已有的 IP 地址，从而导致网络通信的瘫痪。针对这种情况，可以在一个网络中配置两台以上的 DHCP 服务器。当其中一台 DHCP 服务器失效时，由另一台（或几台）DHCP 服务器提供服务，不影响网络的正常运行。最后，如果要在一个由多网段组成的网络中使用 DHCP，则必须在每个网段上各安装一台 DHCP 服务器，或者保证路由器具有前向自举广播的功能。



►► 6.1.2 DHCP 工作原理

当 DHCP 客户端启动时，会自动搜索网络中的 DHCP 服务器，并请求租用 IP 地址。DHCP 服务器会向该客户端提供一个可用的 IP 地址，这样客户端就可以使用该 IP 地址连接网络并与其他计算机通信。下面，以一台计算机自动获取 IP 地址的过程简述 DHCP 的工作原理。

1. 寻找 DHCP 服务器

当 DHCP 客户端第 1 次启动网络组件时，如果发现本机上没有任何 IP 地址等相关参数，则会向网络上发出一个 DHCPDISCOVER 数据包。这个数据包的源地址为 0.0.0.0，而目的地址则为 255.255.255.255，用于广播到整个网络，然后加上 DHCPDISCOVER 的信息向整个网络广播。

在 Windows 的预设情况下，DHCPDISCOVER 的等待时间预设为 1 秒。即当客户端发送第 1 个 DHCPDISCOVER 包之后，如果在 1 秒之内没有得到响应的话，则广播第 2 次 DHCPDISCOVER。如果一直得不到响应，客户端将在 16 秒之内广播 4 次 DHCPDISCOVER。如果仍未得到 DHCP 服务器的响应，客户端则显示错误信息，宣告 DHCPDISCOVER 失败。此时 DHCP 客户端会从 169.254.0.1~169.254.255.254 自动获取一个地址并设置子网掩码为 255.255.0.0，以后系统会继续在 5 分钟之后再重复一次 DHCPDISCOVER 的过程。

2. 提供 IP 租用地址

当 DHCP 服务器收到客户端发出的 DHCPDISCOVER 广播后，它会从可用地址中选择最前面的 IP，连同其他 TCP/IP 设定（包括子网掩码、网关地址、DNS 地址及 WINS 服务器地址等参数）回应给客户端一个 DHCPOFFER 包。

由于客户端在开始时还没有 IP 地址，所以在其 DHCPDISCOVER 包内会带有其 MAC 地址信息，并且有一个 XID 编号来辨别该包。DHCP 服务器返回的 DHCPOFFER 数据包则会根据这些信息传递给要求租约的客户，根据服务器端的设定，DHCP OFFER 包会包含一个租约期限的信息。

3. 接受 IP 租约

如果客户端收到网络上多台 DHCP 服务器的回应，则会从中选择一个 DHCP OFFER（通常是最先到达的那个）。并且会向网络上发送一个 DHCPREQUEST 广播数据包，告诉所有 DHCP 服务器它将指定接受哪一台服务器提供的 IP 地址。

同时，客户端还会向网络发送一个 ARP（Address Resolution Protocol，地址解析协议）包，查询网络中是否有其他机器使用该 IP 地址。如果发现该 IP 已经被占用，客户端则会送出一个 DHCPDECLINE 数据包给 DHCP 服务器，拒绝接受其 DHCP OFFER 并重新发送 DHCPDISCOVER 信息。

4. 租约确认

当 DHCP 服务器接收到客户端的 DHCPREQUEST 之后，会向客户端发出一个 DHCPACK 客户端回应以确认 IP 租约的正式生效，也结束了一个完整的 DHCP 工作过程。

DHCP 服务器分配的 IP 地址是有租约限制的，默认情况下为 8 天。当 DHCP 客户端租约到一半时会发出 DHCPREQUEST，如果此时得不到 DHCP 服务器确认，客户端还可以使用这个 IP 地址；当租约到达 75% 时，如果还得不到确认的话，则客户端就会放弃使用此地址，开始新一轮的申请。

DHCP 服务器以广播方式进行，为此需要在每一个子网中安装一台 DHCP 服务器。如果需要使用一台 DHCP 服务器为所有子网的工作站分配 IP 地址，则需要在每个子网中配置（或安装）DHCP 中继服务器，现在的三层交换机都支持 DHCP 中继。

►► 6.1.3 DHCP 服务器授权

在 Windows 2000 以前版本的网络系统中，只要网络中安装并配置了 DHCP 服务器，网络中的客

户端就可以从这些 DHCP 服务器获得地址。但是如果网络中有多台 DHCP 服务器（有的 DHCP 服务器并不是网络管理员配置的，即“非法的”），那么 DHCP 客户端可能会从“非法的” DHCP 服务器上获得不同地址，从而导致网络通信故障。

为解决这种问题，从 Windows 2000 Server 开始，DHCP 服务器中引入了“授权”功能。要求加入到 Active Directory 的 DHCP 服务器必须在 Active Directory 中经过“授权”，才能对外提供服务并为网络分配 IP 地址。不过，如果 DHCP 服务器并没有加入到 Active Directory，仍然可以在“未授权”的情况下提供服务。

在 Windows Server 2003/2008 系统中改进了这种情况，只要网络中存在 Windows Server 2003/2008 的域控制器，无论 Windows Server 2003/2008 的 DHCP 服务器是否加入到域都必须经过“授权”才能提供 DHCP 服务。如果网络中没有域控制器，则 DHCP 服务器不需授权。

6.1.4 VLAN 与 DHCP 中继问题

现在三层交换机的使用非常普及，许多单位已经用其划分 VLAN，这样可以减少网络的广播并提高网络的使用效率。在划分有 VLAN 的网络中，仍然只需要使用一台或两台 DHCP 服务器，而不需要在每个 VLAN 中部署一台 DHCP 服务器。在前面已经讲到，DHCP 服务是靠“广播”的方式获得 TCP/IP 地址及 TCP/IP 参数的，在“屏幕”广播的 VLAN 之间获得 IP 地址是靠三层交换机的“DHCP Replay (DHCP 中继)”来实现的。在三层交换机中需要在没有 DHCP 服务器的 VLAN 中，启用并配置 DHCP 中继功能并指定网络中 DHCP 服务器的位置（即 DHCP 服务器的 IP 地址）。

DHCP 服务器无须过多其他设置，只需要为每个 VLAN 创建一个作用域并正确设置作用域的参数、网关地址及其他参数（如 DNS 地址及 WINS 服务器地址）即可。

在 Windows 2000 Server 与 Windows Server 2003/2008 操作系统中提供了“DHCP 中继”功能，但在实际使用中并没有多大意义。因为使用三层交换机的成本已经很低，用户无需因为降低成本而使用“普通交换机+Windows Server 软路由”的方式划分 VLAN。并且即使使用 Windows Server 2003/2008 作为“DHCP 中继”，每个 VLAN 中都放置一台计算机也是不现实的。在实际的应用中，Windows Server 2003/2008 中的“DHCP 中继”是在兼做“路由和远程访问”服务器时为了让远程客户端访问内网而使用的，此时作为“DHCP 中继”才有其存在的意义。

6.2 安装 DHCP 服务器

在 Windows Server 2003 系统中可以通过“配置您的服务器向导”或“Windows 组件向导”来安装 DHCP 服务器。在 Windows Server 2008 系统中，则需要在“初始配置任务”或“服务器管理器”中启动“添加角色向导”安装。

6.2.1 安装 DHCP 服务器

安装 DHCP 服务器的操作步骤如下。

① 在“初始配置任务”窗口中单击“添加角色”链接，运行“添加角色向导”。当显示如图 6-1 所示的“选择服务器角色”对话框时，选中“DHCP 服务器”复选框。

② 单击“下一步”按钮，显示如图 6-2 所示的“DHCP 服务器”对话框，其中显示 DHCP 服务器简介信息及相关的注意事项。

③ 单击“下一步”按钮，显示如图 6-3 所示的“选择网络连接绑定”对话框，选择为客户端提供服务的网络连接。

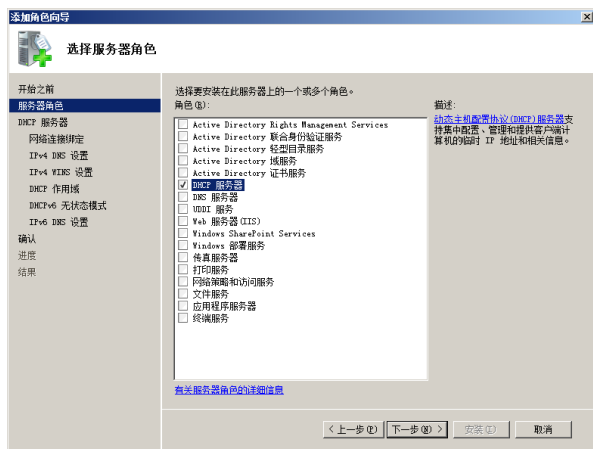


图 6-1 “选择服务器角色”对话框



图 6-2 “DHCP 服务器”对话框

④ 单击“下一步”按钮，显示如图 6-4 所示的“指定 IPv4 DNS 服务器设置”对话框。在“父域”文本框中键入活动目录的域名，在“首选 DNS 服务器 IPv4 地址”和“备用 DNS 服务器 IPv4 地址”文本框中键入本地网络中所使用的 DNS 服务器的 IPv4 地址。

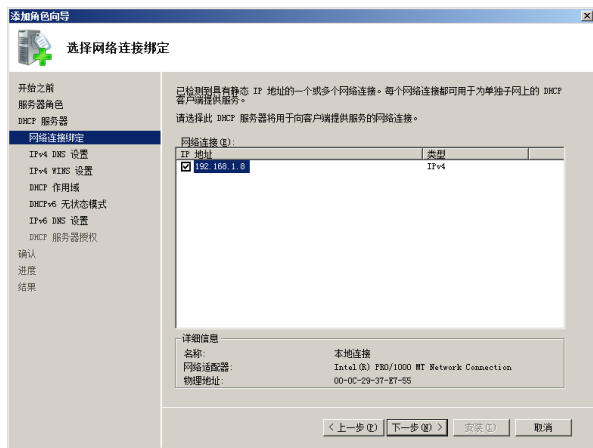


图 6-3 “选择网络连接绑定”对话框

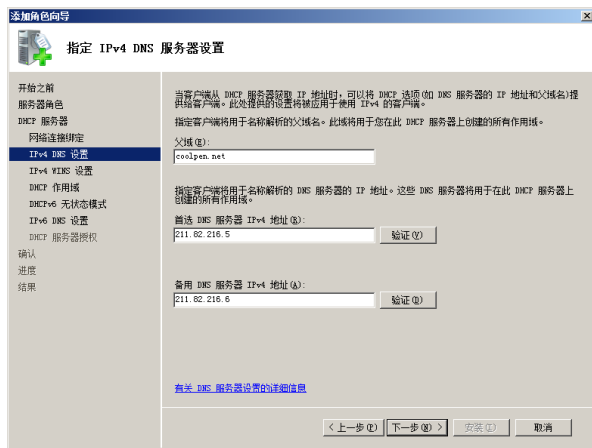


图 6-4 “指定 IPv4 DNS 服务器设置”对话框



提示

虽然 DHCP 没有处于域环境中，但是如果设置 DNS 服务器地址，也必须同时键入父域名称。

⑤ 单击“下一步”按钮，显示如图 6-5 所示的“指定 IPv4 WINS 服务器设置”对话框，选择是否要使用 WINS 服务。

⑥ 单击“下一步”按钮，显示如图 6-6 所示的“添加或编辑 DHCP 作用域”对话框。在其中可添加 DHCP 作用域，并设置为客户端分配的 IP 地址范围，也可以在安装完成后添加。

⑦ 单击“添加”按钮，显示如图 6-7 所示的“添加作用域”对话框。设置该作用域的名称、起始和结束 IP 地址、子网掩码、默认网关，以及子网类型，并选中“激活此作用域”复选框，在作用域创建完成后自动激活；否则需要手动激活。

⑧ 单击“确定”按钮，添加成功一个作用域。单击“下一步”按钮，显示如图 6-8 所示的“配置 DHCPv6 无状态模式”对话框。由于现在不配置 IPv6，因此选择“对此服务器禁用 DHCPv6 无状态模式”单选按钮。

⑨ 单击“下一步”按钮，如果是在 Active Directory 中安装 DHCP 服务器，则显示如图 6-9 所示的“授权 DHCP 服务器”对话框，要求指定授权此 DHCP 服务器的凭据。选择“使用当前凭据”单选

按钮，可以使用当前登录账户授权；如果使用其他账户授权，则选择“使用备用凭据”单选按钮；如果现在不授权，则选择“跳过 AD DS 中此 DHCP 服务器的授权”单选按钮。

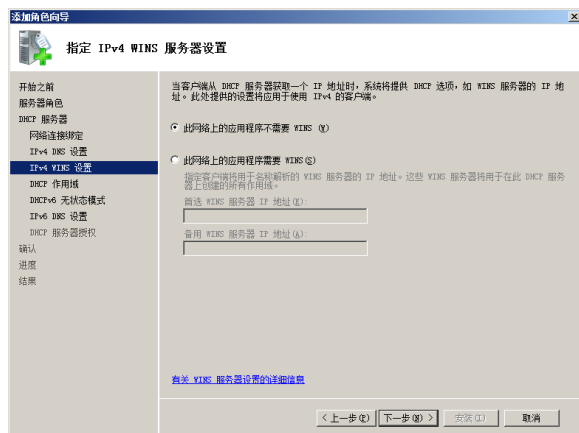


图 6-5 “指定 IPv4 WINS 服务器设置”对话框



图 6-6 “添加或编辑 DHCP 作用域”对话框

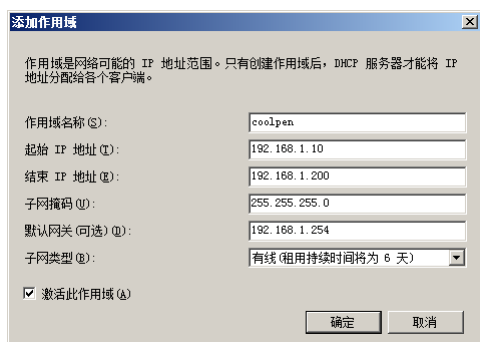


图 6-7 “添加作用域”对话框

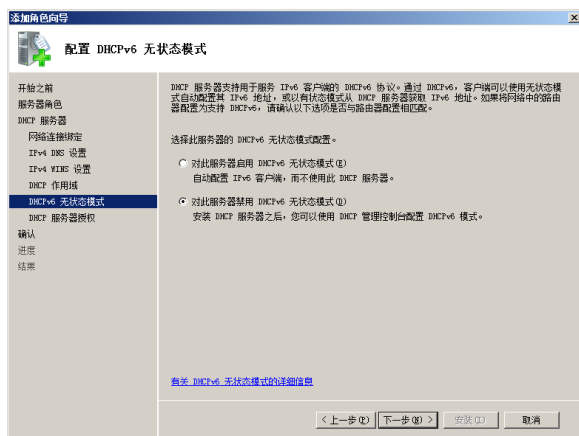


图 6-8 “配置 DHCPv6 无状态模式”对话框



如果现在不授权 DHCP 服务器，则需要安装完成后在 DHCP 控制台中授权。

⑩ 单击“下一步”按钮，显示如图 6-10 所示的“确认安装选择”对话框。其中列出前面所做的配置，如果需要更改，可单击“上一步”按钮返回。

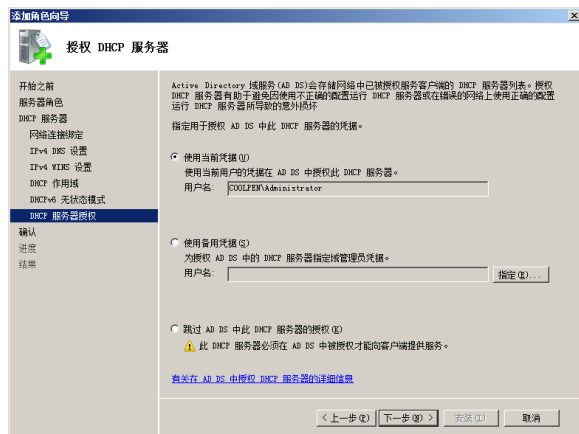


图 6-9 “授权 DHCP 服务器”对话框



图 6-10 “确认安装选择”对话框

⑪ 单击“安装”按钮，开始安装 DHCP 服务器。安装完成后显示如图 6-11 所示的“安装结果”对话框，提示 DHCP 服务器已经安装成功。

⑫ 单击“关闭”按钮关闭向导，DHCP 服务器安装完成。

安装完成 DHCP 服务器以后，单击“开始”→“管理工具”→“DHCP”选项。打开 DHCP 控制台，如图 6-12 所示，在其中可配置和管理 DHCP 服务器。



图 6-11 “安装结果”对话框

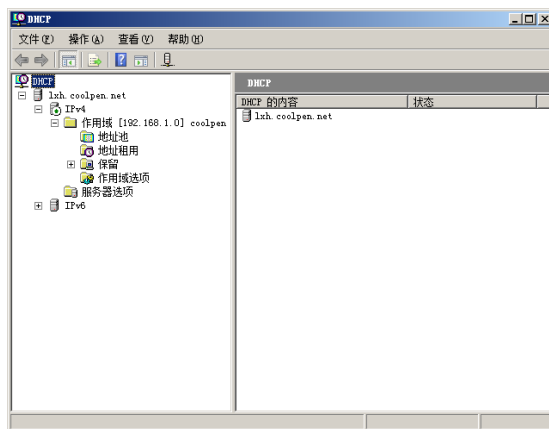


图 6-12 DHCP 控制台

提示 对于规模较大且用户数量较多的大型企业网络，可以采取搭建多台 DHCP 服务器的方法，以提高网络效率。

6.2.2 在 Active Directory 中授权

如果 DHCP 服务器是域的成员，并且在安装 DHCP 服务过程没有选择授权（如图 6-13 所示），那么在安装完成后就必须首先授权才能为客户端提供 IP 地址，而独立服务器不需要授权。

右击 DHCP 服务器名，选择快捷菜单中的“授权”选项，即可为 DHCP 服务器授权。重新打开 DHCP 控制台，即可显示 DHCP 服务器已授权。

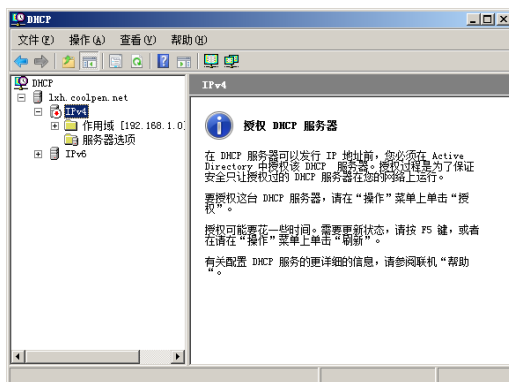


图 6-13 DHCP 服务器未授权

6.2.3 创建作用域

为了向网络中的计算机提供 IP 地址，必须创建作用域。为了向不同网络中提供不同的 IP 地址，还需要创建不同的作用域。并且可以创建超级作用域，以管理多个作用域。

1. 创建作用域

① 打开 DHCP 控制台，展开服务器名。选择“IPv4”选项，右击并选择快捷菜单中的“新建作

用域”选项，打开“新建作用域向导”对话框，如图 6-14 所示。

② 单击“下一步”按钮，显示如图 6-15 所示的“作用域名称”对话框。在“名称”文本框中键入新作用域的名称，以便与其他作用域相区分。

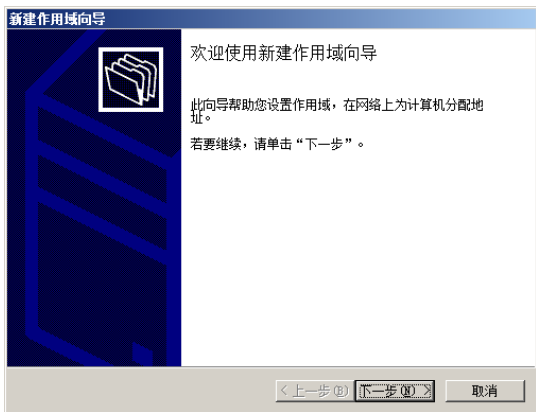


图 6-14 “新建作用域向导”对话框

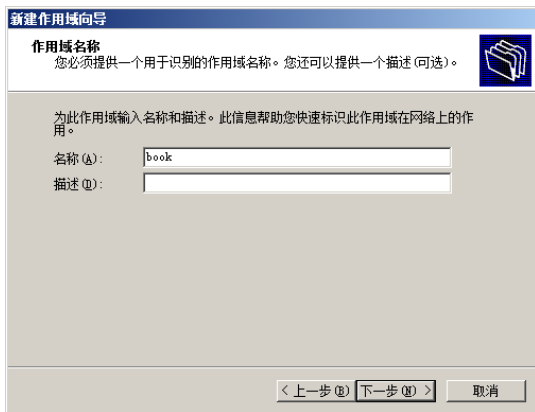


图 6-15 “作用域名称”对话框

③ 单击“下一步”按钮，显示如图 6-16 所示的“IP 地址范围”对话框，在“起始 IP 地址”和“结束 IP 地址”文本框中键入待设置的 IP 地址范围。

④ 单击“下一步”按钮，显示如图 6-17 所示的“添加排除”对话框。在“起始 IP 地址”和“结束 IP 地址”文本框中键入待排除的 IP 地址或 IP 地址段，单击“添加”按钮，将其添加到“排除的地址范围”列表框中。

⑤ 单击“下一步”按钮，显示如图 6-18 所示的“租用期限”对话框，在其中设置客户端从此作用域所租用 IP 地址的时间。

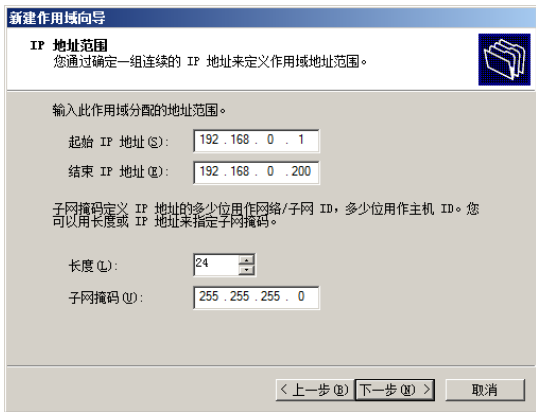


图 6-16 “IP 地址范围”对话框

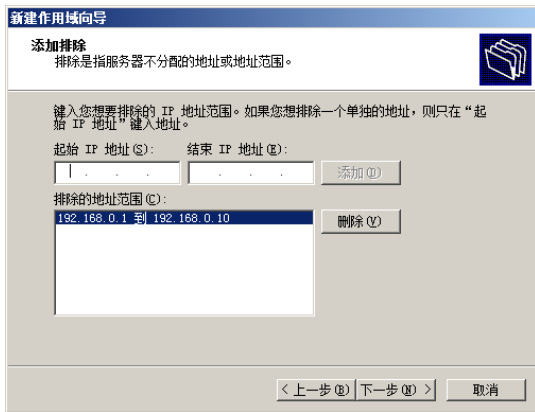


图 6-17 “添加排除”对话框

⑥ 单击“下一步”按钮，显示如图 6-19 所示的“配置 DHCP 选项”对话框。其中提示是否配置 DHCP 选项，选择默认的“是，我想现在配置这些选项”单选按钮。

⑦ 单击“下一步”按钮，显示如图 6-20 所示的“路由器(默认网关)”对话框。在“IP 地址”文本框键入此作用域要分配的网关，单击“添加”按钮将其添加到列表框中。

⑧ 单击“下一步”按钮，显示如图 6-21 所示的“域名称和 DNS 服务器”对话框。在“父域”文本框中键入用来进行 DNS 解析时使用的父域，在“IP 地址”文本框中键入 DNS 服务器的 IP 地址，单击“添加”按钮将其添加到列表框中。

⑨ 单击“下一步”按钮，显示如图 6-22 所示的“WINS 服务器”对话框。在其中设置 WINS 服务器，如果网络中没有配置 WINS 服务器，则不必设置。

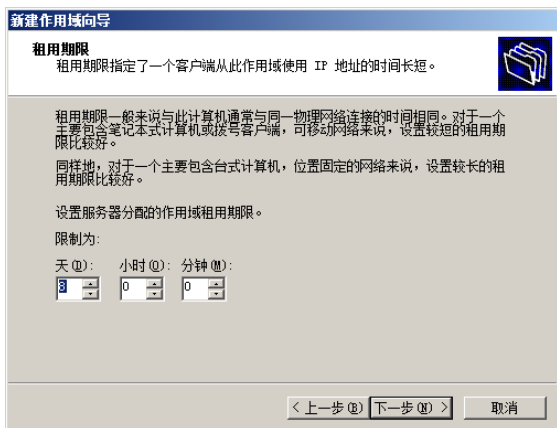


图 6-18 “租用期限”对话框

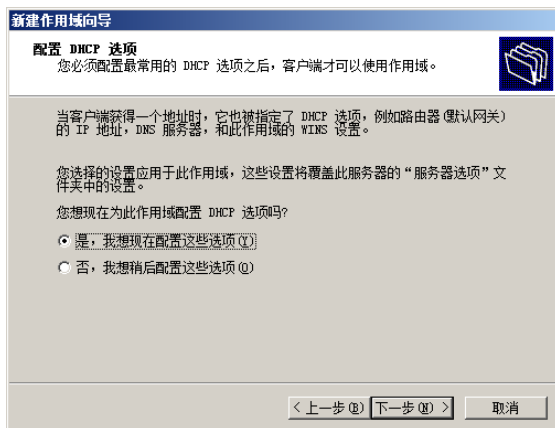


图 6-19 “配置 DHCP 选项”对话框

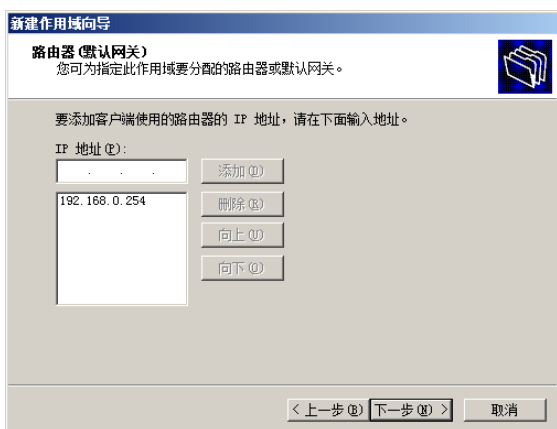


图 6-20 “路由器（默认网关）”对话框

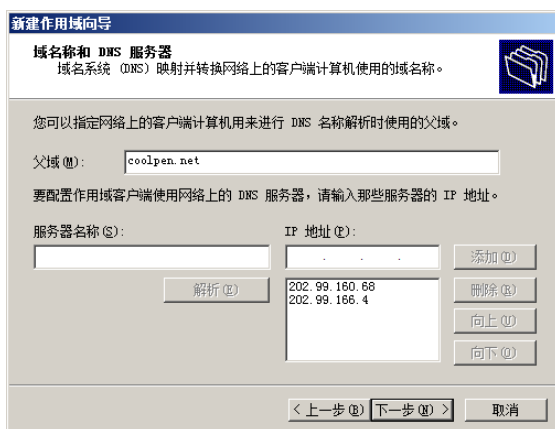


图 6-21 “域名称和 DNS 服务器”对话框

⑩ 单击“下一步”按钮，显示如图 6-23 所示的“激活作用域”对话框。提示是否激活作用域，选择默认的“是，我想现在激活此作用域”单选按钮。

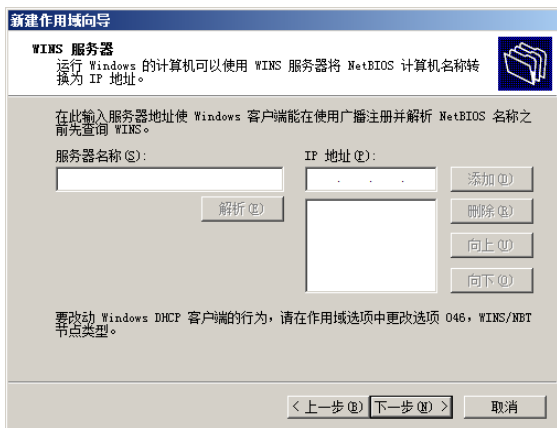


图 6-22 “WINS 服务器”对话框

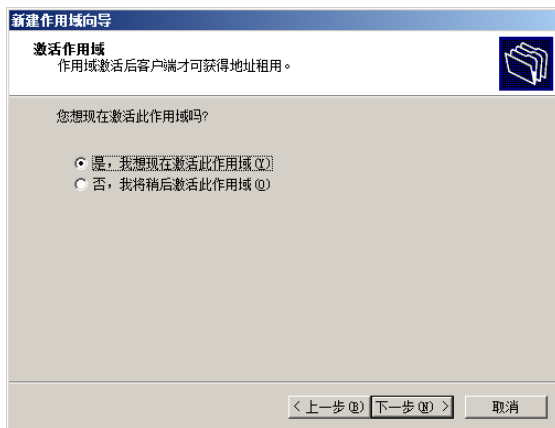


图 6-23 “激活作用域”对话框

⑪ 单击“下一步”按钮，显示如图 6-24 所示的“正在完成新建作用域向导”对话框。

⑫ 单击“完成”按钮，创建完成作用域并自动激活，按照同样步骤可以创建多个作用域。

2. 创建超级作用域

自 Windows Server 2003 起增加了超级作用域功能，可以将 DHCP 服务器中的多个作用域组成超级作用域作为单个实体来管理，通常用于多网配置。所谓多网，是指在同一物理网段上使用多台 DHCP

服务器管理分离的逻辑 IP 网络。在多网配置中，可以使用 DHCP 超级作用域来组合并激活网络上使用的 IP 地址的单独作用域范围。通过这种方式，DHCP 服务器可为单个物理网络中的客户端激活并提供来自多个作用域的租约。

① 在 DHCP 控制台展开 DHCP 服务器，右击“IPv4”选项并选择快捷菜单中的“新建超级作用域”选项，打开“新建超级作用域向导”对话框，如图 6-25 所示。

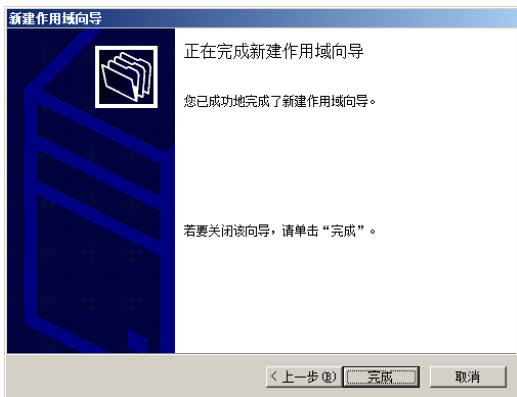


图 6-24 “正在完成新建作用域向导”对话框

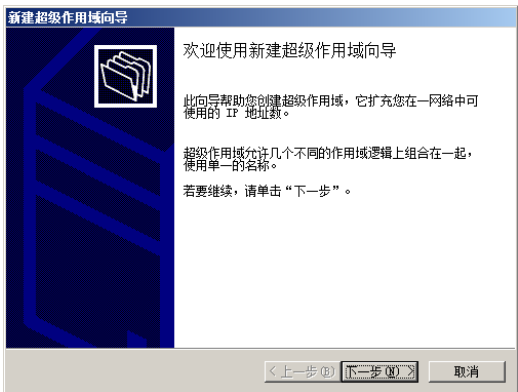


图 6-25 “新建超级作用域向导”对话框

② 单击“下一步”按钮，显示如图 6-26 所示的“超级作用域名”对话框，为超级作用域名键入一个名称。

③ 单击“下一步”按钮，显示如图 6-27 所示的“选择作用域”对话框。在“可用作用域”列表框中选择待添加至超级作用域中的 IP 作用域，可借助 Ctrl 键或 Shift 键选择多个。

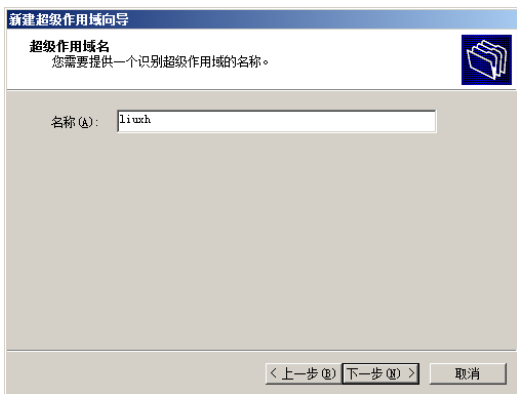


图 6-26 “超级作用域名”对话框

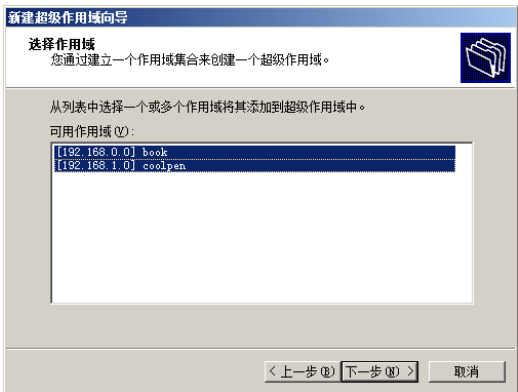


图 6-27 “选择作用域”对话框

④ 单击“下一步”按钮，显示如图 6-28 所示的“正在完成新建超级作用域向导”对话框。

⑤ 单击“完成”按钮，创建成功超级作用域并显示在 DHCP 控制台窗口中，如图 6-29 所示。原有的作用域就像是超级作用域的下一级目录，便于分类管理。

如果之后又新创建了作用域，也可以添加到现有的超级作用域中统一管理。右击新创建的作用域，选择快捷菜单中的“添加到超级作用域”选项，显示如图 6-30 所示的“将作用域 xxx 添加到一个超级作用域”对话框。选择超级作用域名称，单击“确定”按钮即可。

提示 也可以右击超级作用域名称，选择快捷菜单中的“新建作用域”选项来创建新的作用域并自动添加到超级作用域中。

如果要删除超级作用域，则右击待删除的超级作用域名称。选择快捷菜单中的“删除超级作用域”选项，显示如图 6-31 所示的提示框，单击“是”按钮即可删除。需要注意的是删除超级作用域时，原

有的子作用域不会被删除。



图 6-28 “正在完成新建超级作用域向导”对话框

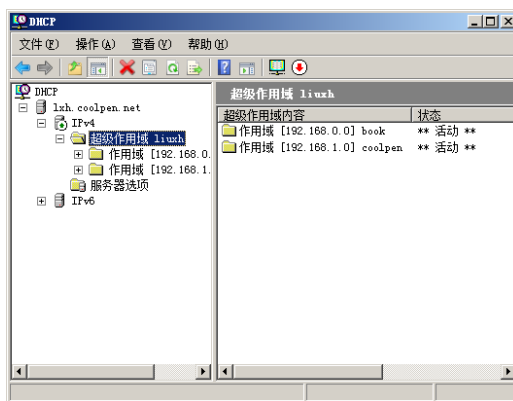


图 6-29 创建成功的超级作用域

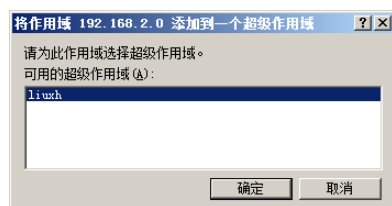


图 6-30 “添加到超级作用域”对话框

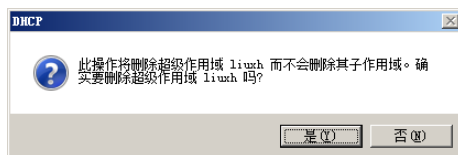


图 6-31 提示框

6.2.4 创建保留地址

在网络中有些特殊的 DHCP 客户端需要分配固定专用的 IP 地址，为此可以利用 DHCP 服务器的“保留”功能来实现，如 Web、FTP 及 E-mail 服务器等。设置为“保留”IP 地址以后，该客户端每次向 DHCP 服务器请求获得 IP 地址或更新 IP 地址的租期时，DHCP 服务器都会为其分配相同的 IP 地址，而其他客户端不会获得该 IP 地址。



注意：

如果在包含保留 IP 地址的作用域中配置了多台 DHCP 服务器，则必须在每台 DHCP 服务器上均生成和复制客户端保留；否则保留的客户端计算机在请求 IP 地址时可能会接收到多台 DHCP 服务器的响应，从而接收到多个不同的 IP 地址。



(1) 在 DHCP 控制台窗口中展开要添加保留 IP 地址的作用域，选择“保留”选项，显示如图 6-32 所示。



图 6-32 选择“保留”选项

(2) 右击“保留”并选择快捷菜单中的“新建保留”选项，显示如图 6-33 所示的“新建保留”对话框。

在其中设置如下选项。

“保留名称”：设置名称，仅用于区分其他保留项。


“IP 地址”：输入保留的 IP 地址。

“MAC 地址”：输入保留的客户端网卡的 MAC，在 Windows 98/Me 系统中可通过运行 winipcfg 命令获得；在 Windows 2000/XP/2003/2008 系统中可以运行 getmac 命令获得。


支持的类型：客户端所支持 DHCP 服务类型，其中 BOOTP 是针对早期的无盘工作站设计的，普通计算机可选择“仅 DHCP”或者“两者”单选按钮。

(3) 单击“添加”按钮，设置的 IP 地址指定给该 DHCP 客户端，如图 6-33 所示。重复操作，可添加多个保留 IP 地址。

设置完成保留 IP 地址后，当 DHCP 客户端向 DHCP 服务器请求获得 IP 地址时，服务器就会检测客户端的 MAC 地址。如果与保留 IP 地址中设置的 MAC 相同，则将保留的 IP 地址分配给该客户端。而其他计算机则不能获得该保留地址。


注意：

设置保留地址以后不能直接修改，如果需要修改，必须首先删除现有的保留地址，然后重新添加。



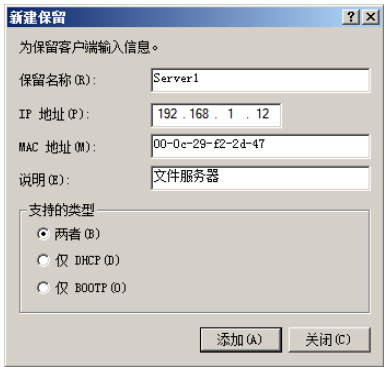


图 6-33 “新建保留”对话框

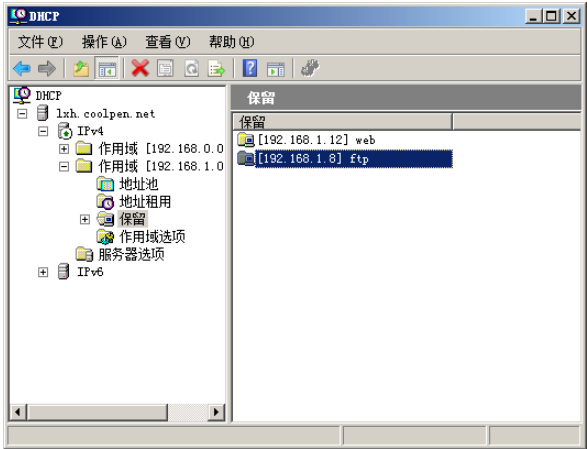


图 6-34 保留 IP 地址

6.3 管理 DHCP 服务器

DHCP 服务器除了可以为 DHCP 客户端提供 IP 地址外，还可设置 DHCP 客户端启动时的工作环境，如登录的域名称、DNS 服务器、WINS 服务器、路由器及默认网关等。在客户端启动或更新租约时，DHCP 服务器可以自动设置其启动后的 TCP/IP 环境。

6.3.1 管理作用域

创建完成作用域以后，有时需要根据需要更改 IP 地址范围及租用期限等，这些都可以在 DHCP 控制台中完成。

(1) 右击要管理的作用域，选择快捷菜单中的“属性”选项，显示如图 2-35 所示“作用域 属性”对话框。默认为“常规”选项卡，在其中可以更改作用域的名称、IP 地址范围及客户端租用期限。

(2) 打开“DNS”选项卡，如图 6-36 所示，在其中设置客户端的 DNS 动态更新方式。

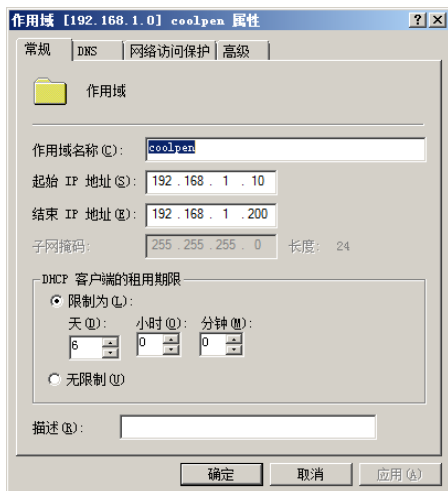


图 6-35 “作用域 属性”对话框

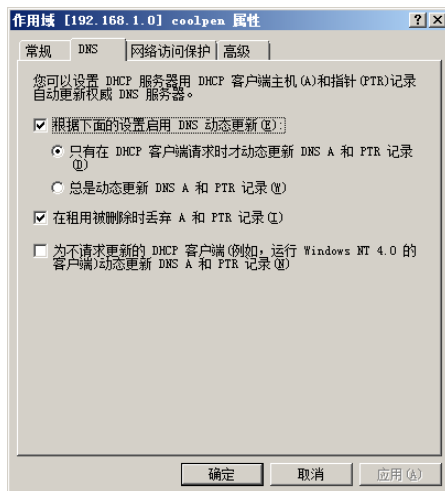


图 6-36 “DNS”选项卡

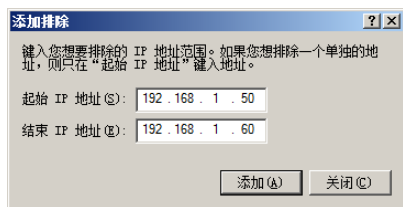


图 6-37 “添加排除”对话框

(3) 设置完成后, 单击“确定”按钮。

如果需要将作用域中的一部分 IP 地址排除, 即不分配给客户端, 则展开作用域。右击“地址池”并选择快捷菜单中的“添加排除范围”选项, 显示如图 6-37 所示的“添加排除”对话框。键入待排除的起始和结束 IP 地址, 单击“添加”按钮即可。已添加的排除地址不能直接更改, 只能删除原来的排除地址, 然后添加新的排除地址。

6.3.2 备份与还原 DHCP 服务器

任何服务都不能避免意外故障的发生, DHCP 服务器也不例外。如果 DHCP 服务器一旦出现故障, 那么不仅客户端不能获得 IP 地址信息, 而且原来的作用域及保留 IP 地址等设置都会丢失, 从而影响到网络的正常使用。因此配置 DHCP 服务器以后, 必须及时备份, 以便出现故障时还原。DHCP 服务器会自动在 %Systemroot%\System32\Dhcp 目录下创建数据库文件, 通过备份还原这些文件即可达到备份还原的目的。

1. 备份数据库

DHCP 服务器的设置数据保存在 \Windows\System32\dhcp 文件夹中, 如图 6-38 所示。其中 dhcp.mdb 为存储数据库文件, 其他文件是辅助文件, 但对 DHCP 服务器的正常工作起着非常重要的作用。另外还有一个 backup 文件夹, 用来备份 DHCP 数据库, DHCP 服务默认会每隔 60 分钟自动将 DHCP 数据库文件备份到该文件夹中。

要备份 DHCP 服务器数据, 只需备份 backup 文件夹及其所有文件。也可以在 DHCP 控制台中选择服务器名, 右击并选择快捷菜单中的“备份”选项, 显示如图 6-39 所示的“浏览文件夹”对话框。选择一个保存路径, 单击“确定”按钮, 即可将 DHCP 服务器中的数据备份到该目录中。



注意：

为了保证所备份数据的完整, 在备份前应在 DHCP 控制台中右击服务器名称, 选择快捷菜单中的“所有任务”→“停止”选项将 DHCP 服务器停止。



2. 还原数据库

DHCP 服务器在每次启动时都会自动检查 DHCP 数据库是否损坏, 如果发现损坏, 将自动使用

\\Windows\\System32\\dhcp\\backup 文件夹内的数据还原。如果 backup 文件夹中的数据也被损坏,那么系统将无法自动完成还原工作,无法提供相关的服务。

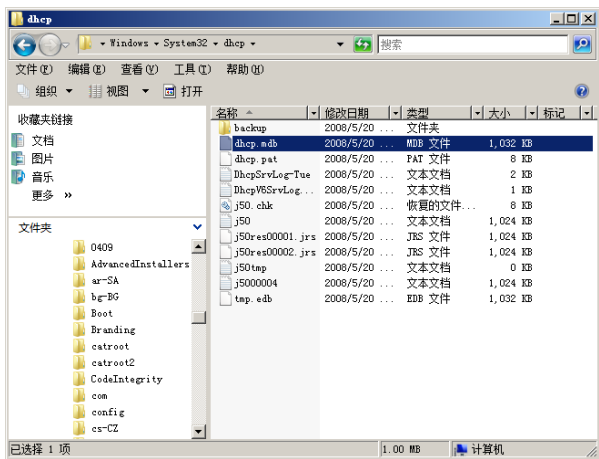


图 6-38 DHCP 数据库文件

为还原 DHCP 数据库文件,打开 DHCP 控制台。右击服务器名,选择快捷菜单中的“还原”选项,显示如图 6-40 所示的“浏览文件夹”对话框。选择保存备份文件的目录,单击“确定”按钮即可还原 DHCP 服务器数据。然后重新启动 DHCP 服务器,即可自动使用复制的数据还原。

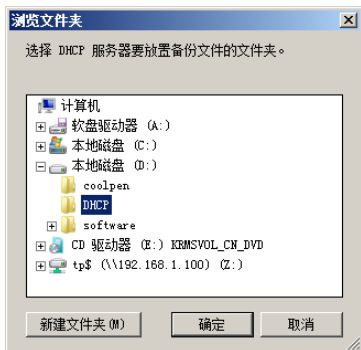


图 6-39 备份 DHCP

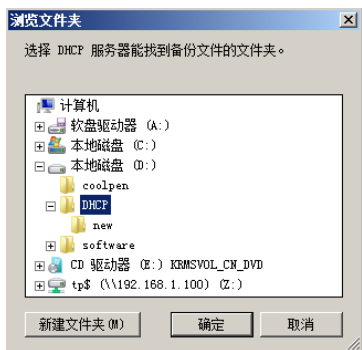


图 6-40 还原 DHCP



注意：在还原 DHCP 服务器数据前也必须停止 DHCP 服务器。

6.3.3 迁移 DHCP 服务器

在网络中可能需要使用一台新的 DHCP 服务器更换原有的 DHCP 服务器,或者需要使用其他服务器运行 DHCP 服务,为此需要重新配置服务器。重新设置不仅麻烦,而且也可能会因不慎而丢失数据。通常,网络管理员可以备份原来 DHCP 服务器中的数据库,然后迁移到新的 DHCP 服务器中。这样可以保证 DHCP 服务器数据不丢失,而且设置也简单。

1. 备份旧 DHCP 服务器中的数据

在原来的 DHCP 服务器执行如下操作备份 DHCP 数据。

- ① 在 DHCP 控制台中选择 DHCP 服务器名称,右击并选择快捷菜单中的“所有任务”→“停止”选项,或者运行“net stop dhcpserver”命令将 DHCP 服务器停止。
- ② 将\\Windows\\System32\\dhcp 文件夹下的所有文件及文件夹全部备份到其他磁盘中。

③ 在 DHCP 服务器上运行注册表命令 `regedit.exe`，打开如图 6-41 所示的“注册表编辑器”窗口依次展开分支 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPserver`。

④ 右击“DHCPserver”选项，选择快捷菜单中的“导出”选项，显示如图 6-42 所示的“导出注册表文件”对话框。选择一个保存位置，并在“文件名”文本框中键入一个名称，在“导出范围”选项组中选择“所选分支”单选按钮。

⑤ 单击“保存”按钮，将该分支导出为注册表文件。

⑥ 将旧 DHCP 服务器中的 DHCP 服务卸载，并将 `\Windows\System32\dhcp` 文件夹下的所有文件删除。

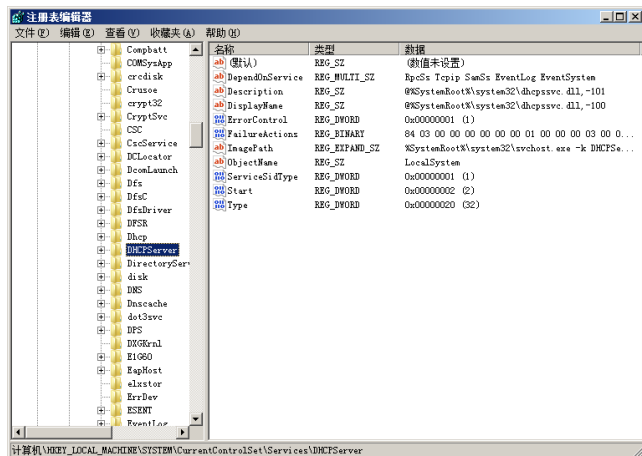


图 6-41 “注册表编辑器”窗口

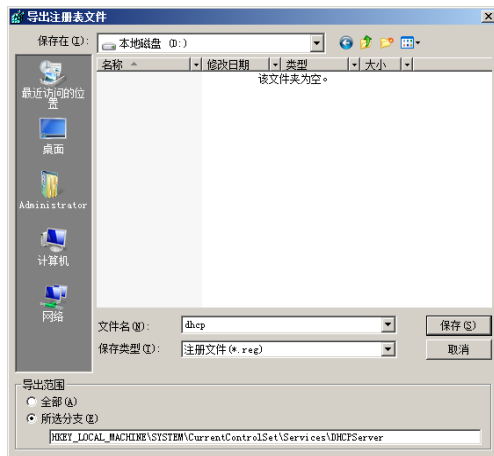


图 6-42 “导出注册表文件”对话框

2. 将数据添加到新的 DHCP 服务器中

在新的 DHCP 服务器中安装 DHCP 服务，然后执行以下操作步骤将旧 DHCP 服务器中备份的数据迁移到新 DHCP 服务器中。

① 停止 DHCP 服务。

② 将旧 DHCP 服务器中备份的所有文件全部复制到新 DHCP 服务器的 `\Windows\System32\dhcp` 文件夹中，并将备份的注册表文件复制到新 DHCP 服务器中。

③ 在新 DHCP 服务器上运行 `regedit.exe` 命令打开“注册表编辑器”窗口，依次展开分支 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPserver`。然后双击在旧服务器上导出的注册表文件，或者右击并选择快捷菜单中的“合并”选项，显示如图 6-43 所示的警告框。

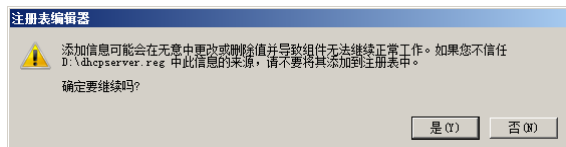


图 6-43 警告框

④ 单击“是”按钮将导出的注册表文件导入到注册表中。

⑤ 重新打开 DHCP 控制台，右击 DHCP 服务器名称。选择快捷菜单中的“所有任务”→“启动”选项，或者运行 `net start dhcpserver` 命令，启动 DHCP 服务器。

⑥ 在 DHCP 控制台中右击“IPv4”选项并选择快捷菜单中的“协调所有作用域”选项，显示如图 6-44 所示的“协调所有作用域”对话框。

⑦ 单击“验证”按钮，开始验证所有作用域。完成后显示如图 6-45 所示的提示框，单击“确定”按钮即可。

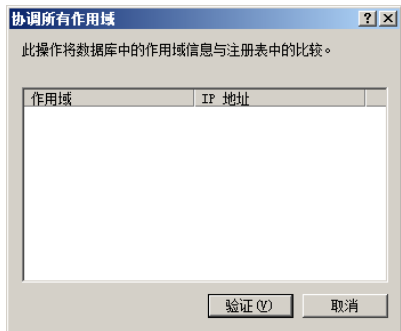


图 6-44 “协调所有作用域”对话框



图 6-45 提示框

通过以上的设置，即可将 DHCP 服务迁移到新的 DHCP 服务器中并正常投入运行。

6.3.4 跨网段的 DHCP 服务器

由于 DHCP 依赖于广播信息，因此通常应将 DHCP 客户端和 DHCP 服务器位于同一个网段之内。但网络中经常需要划分多个网段，而 DHCP 不能跨网段操作。因此可在一两个网段中部署一台~两台 DHCP 服务器，而在其他网段使用 DHCP 中继代理。

1. DHCP 中继的原理

使用 DHCP 中继代理可以使 DHCP 请求能够从一个网段传递到另一个网段，但必须遵循以下要求。

- (1) 在路由网络中，一台 DHCP 服务器必须至少位于一个网段中。
- (2) 必须使用路由器或计算机作为 DHCP 和 BOOTP 中继代理服务器以支持网段之间 DHCP 通信的转发。

不同网段依靠路由器连接，而路由器本身会阻断 LAN 广播，这样没有部署 DHCP 服务器的网段就无法向部署有 DHCP 服务器的网段发出 DHCP 地址请求。要解决这个问题，需要添加一个 DHCP 中继代理服务器。当没有 DHCP 服务器的网段中的客户端发出 DHCP 请求时，DHCP 中继代理就会像 DHCP 服务器一样接收广播。然后向另一网段的 DHCP 服务器发出单播请求，这样就可以获得 IP 地址。

DHCP 中继代理有两种解决方案，一种方案是路由器必须支持 DHCP/BOOTP 中继代理功能（符合 RFC 1542 规范），能够中转 DHCP 和 BOOTP 通信，现在多数路由器或三层交换机都支持 DHCP 中继代理；另一种方案路由器不支持 DHCP/BOOTP 中继代理，则可以在一台运行 Windows Server 2000/2003/2008 的计算机中安装 DHCP 中继代理组件，不能在 DHCP 服务器上配置 DHCP 代理。

中继代理将其连接的其中一个物理接口（如网卡）上广播的 DHCP/BOOTP 消息中转到其他物理接口连接的远程子网。

2. 配置 DHCP 中继代理服务

首先要在 Windows Server 2008 中配置网络地址转换器（NAT），即安装路由和远程访问服务器。

① 运行“添加角色向导”，在如图 6-46 所示的“选择服务器角色”对话框中选中“网络策略和访问服务”复选框。

② 单击“下一步”按钮，显示如图 6-47 所示的“网络策略和访问服务”对话框，其中列出网络策略和访问服务的概述信息。

③ 单击“下一步”按钮，显示如图 6-48 所示的“选择角色服务”对话框，选中“路由和远程访问服务”复选框。

④ 单击“下一步”按钮，显示如图 6-49 所示的“确认安装选择”对话框，其中列出待安装的角色。

⑤ 单击“安装”按钮开始安装。完成后显示如图 6-50 所示的“安装结果”对话框，提示安装完成。

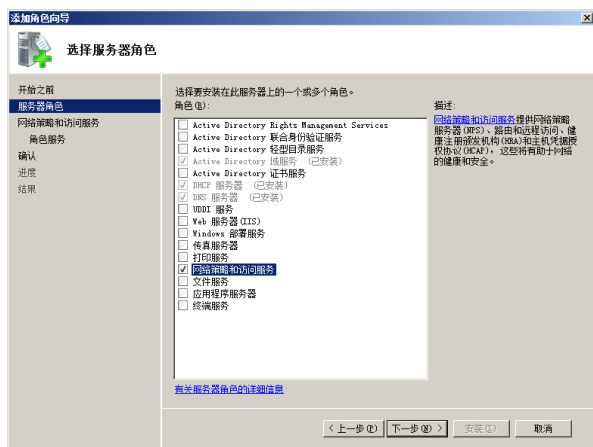


图 6-46 “选择服务器角色”对话框



图 6-47 “网络策略和访问服务”对话框

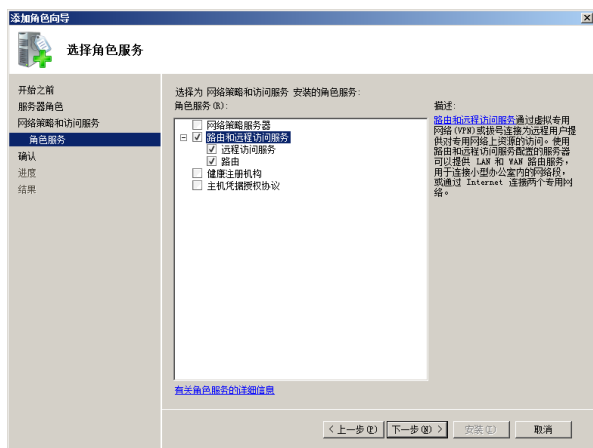


图 6-48 “选择角色服务”对话框

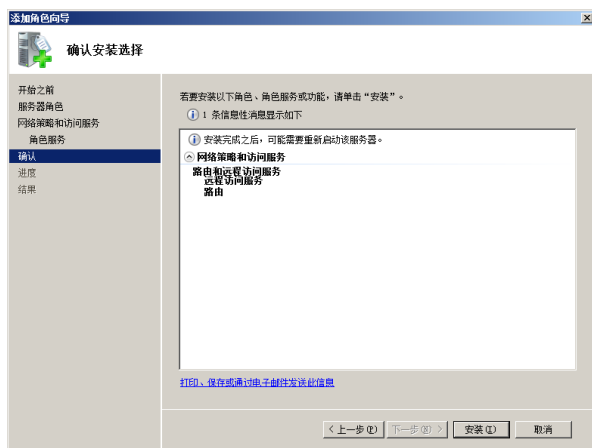


图 6-49 “确认安装选择”对话框

⑥ 单击“关闭”按钮关闭向导，单击“开始”→“管理工具”→“路由和远程访问”选项，显示如图 6-51 所示的“路由和远程访问”窗口。

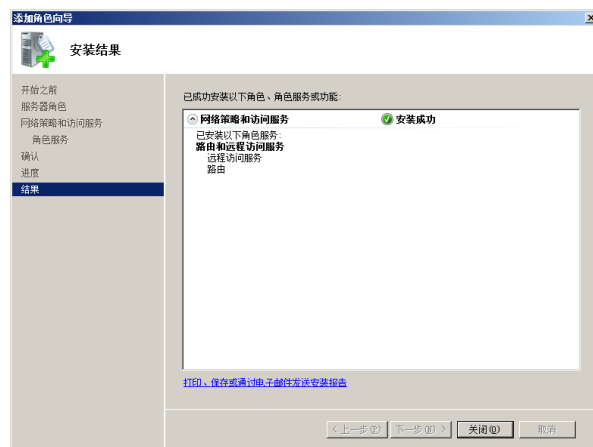


图 6-50 “安装结果”对话框

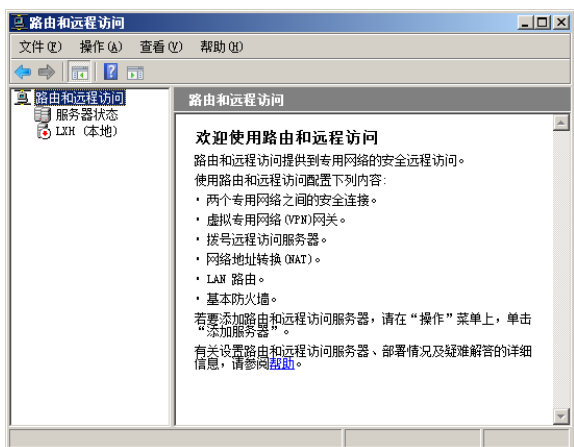


图 6-51 “路由和远程访问”窗口

⑦ 右击服务器名，选择快捷菜单中的“配置并启用路由和远程访问”选项。打开“路由和远程访问服务器安装向导”对话框，如图 6-52 所示。

⑧ 单击“下一步”按钮，显示如图 6-53 所示的“配置”对话框，选择“网络地址转换 (NAT)”单选按钮。

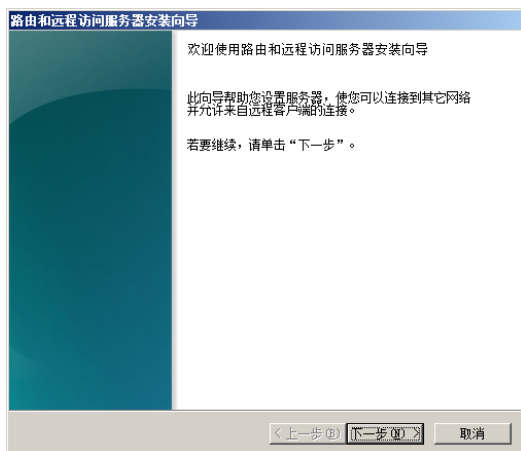


图 6-52 “路由和远程访问服务器安装向导”对话框

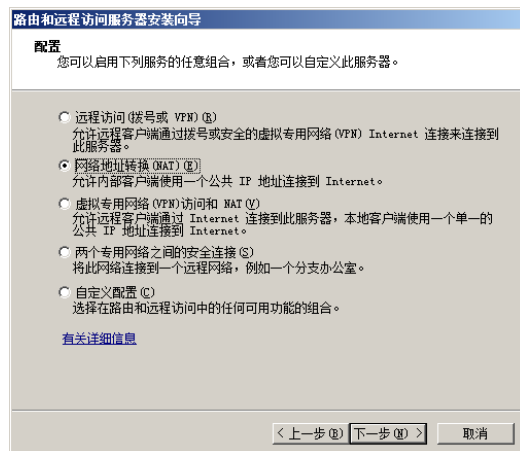


图 6-53 “配置”对话框

⑨ 单击“下一步”按钮，显示如图 6-54 所示的“NAT Internet 连接”对话框。选择“使用此公共接口连接到 Internet”单选按钮，并在“网络接口”列表框中选择连接到 Internet 的本地连接。

⑩ 单击“下一步”按钮，显示如图 6-55 所示的“正在完成路由和远程访问服务器安装向导”对话框。

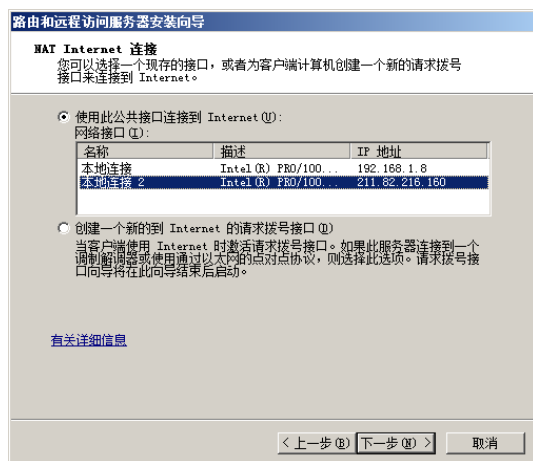


图 6-54 “NAT Internet 连接”对话框

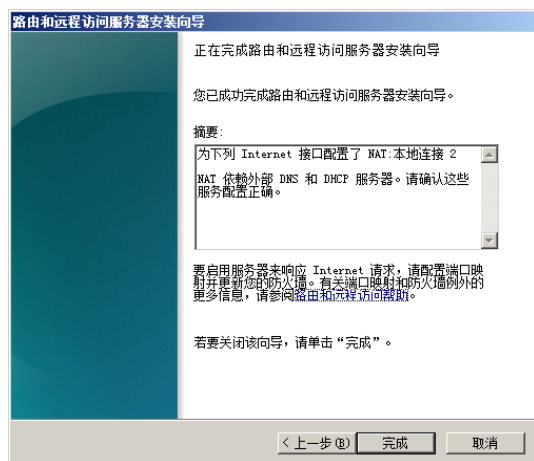


图 6-55 “正在完成路由和远程访问服务器安装向导”对话框

⑪ 单击“完成”按钮，安装完成路由和远程访问，如图 6-56 所示。

⑫ 依次展开“LXH (本地)”→“IPv4”选项，右击“常规”选项并选择快捷菜单中的“新增路由由协议”选项，显示如图 6-57 所示的“新路由协议”对话框。

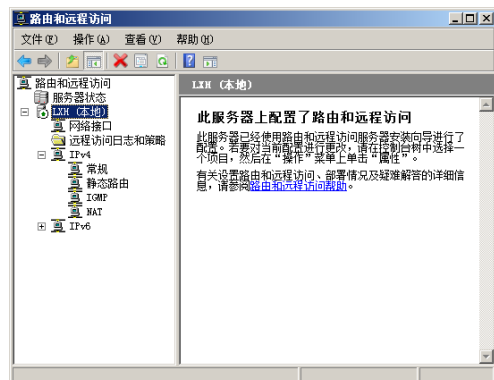


图 6-56 安装完成路由和远程访问

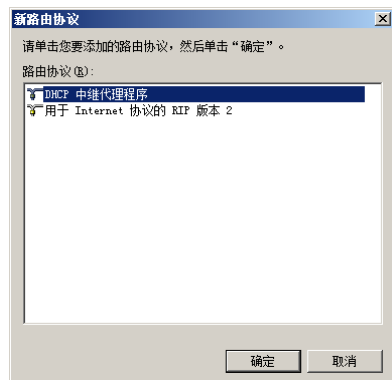


图 6-57 “新路由协议”对话框

⑬ 在“路由协议”列表框中选择“DHCP 中继代理程序”选项，单击“确定”按钮，在“IPv4”目录中添加一个“DHCP 中继代理程序”选项，如图 6-58 所示。

⑭ 右击“DHCP 中继代理程序”选项，选择快捷菜单中的“属性”选项，显示如图 6-59 所示的“DHCP 中继代理程序 属性”对话框。在“服务器地址”文本框中键入 DHCP 服务器的 IP 地址，单击“添加”按钮将其添加到列表框中，可添加多个 DHCP 服务器的 IP 地址。

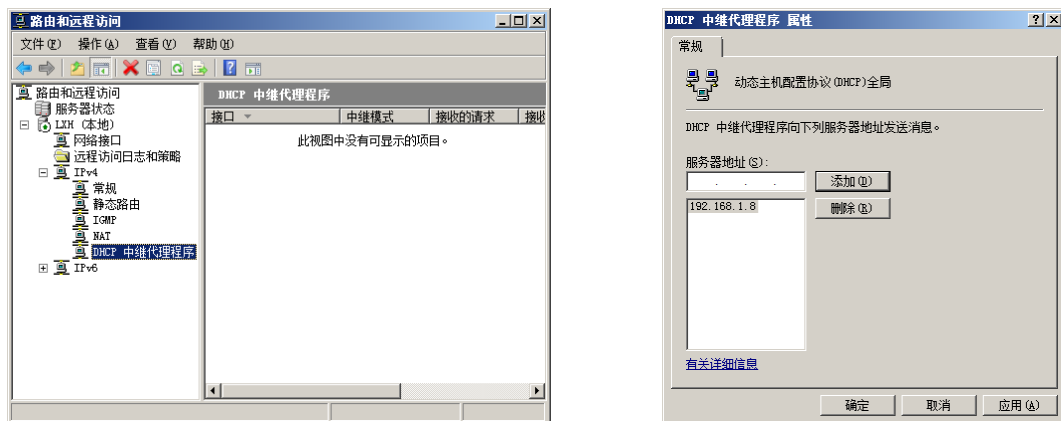


图 6-58 在“IPv4”目录中添加一个“DHCP 中继代理程序”选项 图 6-59 “DHCP 中继代理程序 属性”对话框

⑮ 单击“确定”按钮，右击“DHCP 中继代理程序”选项并选择快捷菜单中的“新增接口”选项。显示如图 6-60 所示“DHCP 中继代理程序的新接口”对话框，选择连接局域网的本地连接。

⑯ 单击“确定”按钮，显示如图 6-61 所示的“DHCP 中继站属性-本地连接 属性”对话框。

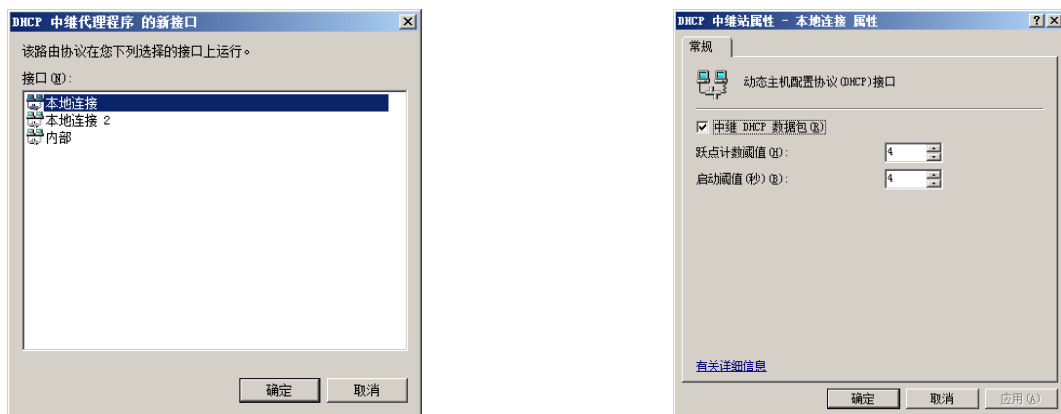


图 6-60 “DHCP 中继代理程序的新接口”对话框

图 6-61 “DHCP 中继站属性-本地连接 属性”对话框

选中“中继 DHCP 数据包”复选框并设置如下阈值。

跃点计数阈值：DHCP 中继代理程序允许 DHCP 信息中转的最大次数，若超过，则忽略此 DHCP 信息。

启动阈值：设置 DHCP 中继代理程序发送 DHCP 信息的等待时间，目的是让本地 DHCP 服务器首先响应此 DHCP 信息。

⑰ 单击“确定”按钮添加该接口，如图 6-62 所示。

至此，创建完成 DHCP 中继代理服务器。

3. 在交换机上配置 DHCP 代理

由于所有 Cisco 二层和三层交换机都支持 DHCP 代理，因此只需简单设置即可实现跨 VLAN 的 DHCP 服务。

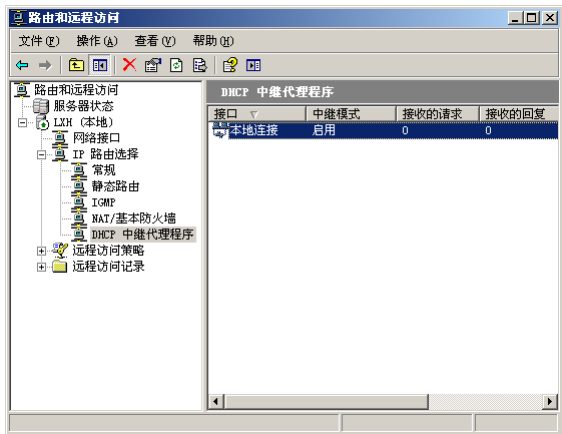


图 6-62 添加的接口

在 Cisco 交换机上执行以下操作。

(1) 启用 DHCP 中继代理:

```
Switch(Config)#service dhcp
Switch(Config)#ip dhcp relay information option
```

(2) 分别在各个 VLAN 中指定 DHCP 服务器地址, 不必指定 DHCP 服务器所在的 VLAN:

```
Switch(Config-vlan)#ip helper-address DHCP_IP_Address
```

6.4 设置并使用 DHCP 客户端

配置 DHCP 服务器以后, 客户端只需设置为“自动获得 IP 地址”即可自动从 DHCP 服务器获取 IP 地址信息并实现网络通信。当然不同操作系统的设置方式也不同。

6.4.1 为 Windows 2000/XP 系统启用 DHCP 客户端

Windows 2000 和 Windows XP 系统启用 DHCP 功能的操作方法完全相同, 这里以 Windows XP 为例介绍。

- ① 右击“网上邻居”图标, 选择快捷菜单中的“属性”选项, 显示如图 6-63 所示的“网络连接”窗口。
- ② 选择“本地连接”图标, 右击并选择快捷菜单中的“属性”选项, 显示如图 6-64 所示“本地连接 属性”对话框。

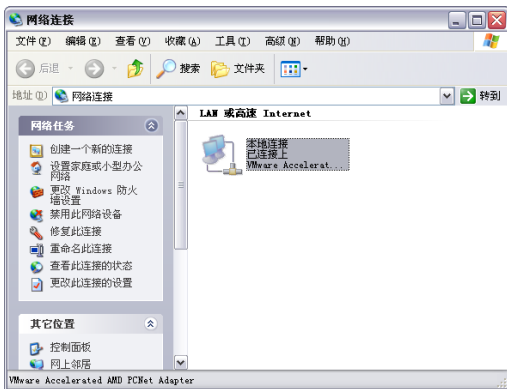


图 6-63 “网络连接”窗口

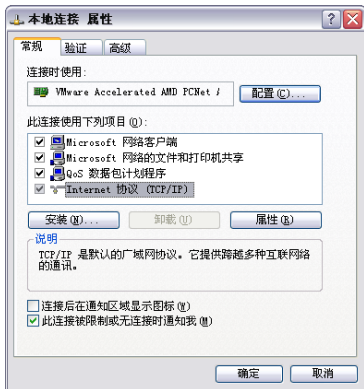


图 6-64 “本地连接 属性”对话框

- ③ 在“此连接使用下列项目”列表框中选择“Internet 协议 (TCP/IP)”选项, 单击“属性”按

钮，显示如图 6-65 所示的“Internet 协议（TCP/IP）属性”对话框，选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”单选按钮。

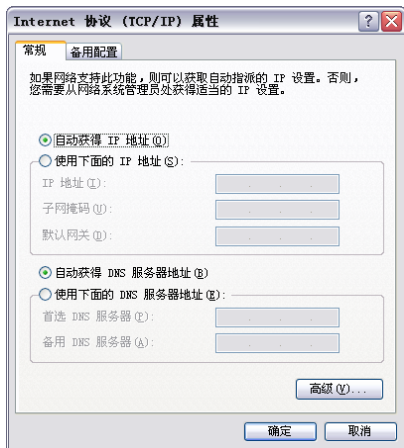


图 6-65 “Internet 协议（TCP/IP）属性”对话框

④ 依次单击“确定”和“关闭”按钮，系统每次启动时都会自动搜索网络中的 DHCP 服务器并获取 IP 地址。

依次单击“开始”→“所有程序”→“附件”→“命令提示符”选项，打开命令提示符窗口。运行 ipconfig /all 命令即可查看是否从 DHCP 服务器获取 IP 地址，如图 6-66 所示。

如果未能从 DHCP 服务器获取有效的 IP 地址，则运行 ipconfig /release 命令释放现有的 IP 地址。然后运行 ipconfig /renew 命令重新获得 IP 地址，如图 6-67 所示。

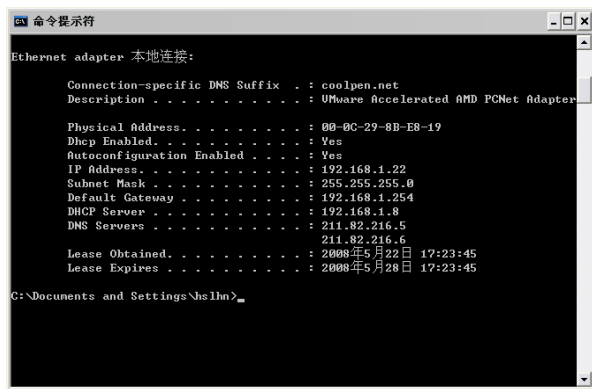


图 6-66 查看是否获取 IP 地址

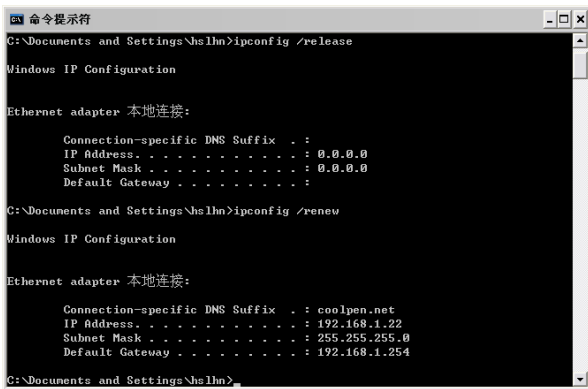


图 6-67 重新获得 IP 地址

提示 如果因网络或 DHCP 服务器故障而导致客户端不能获得 IP 地址，那么 Windows 系统就会自动分配一个 169.254.x.x 的地址。此时应当检查网络，然后释放并重新获得 IP 地址。

6.4.2 为 Windows Vista 系统启用 DHCP 客户端

为 Windows Vista 系统启用 DHCP 客户端的操作步骤如下。

- ① 右击桌面托盘区域的网络图标，选择快捷菜单中的“网络和共享中心”选项，打开“网络和共享中心”窗口。在左侧的“任务”列表中单击“管理网络连接”超级链接，打开“网络连接”图标。
- ② 右击“本地连接”图标，显示如图 6-68 所示的“本地连接 属性”对话框。
- ③ 选择“Internet 协议版本 4 (TCP/IPv4)”选项，单击“属性”按钮。显示如图 6-69 所示的“Internet 协议版本 4 (TCP/IPv4) 属性”对话框，选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”单选按钮。

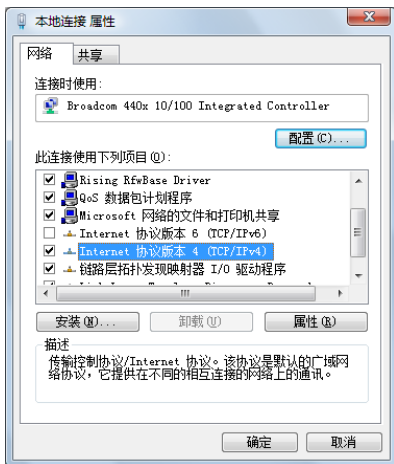


图 6-68 “本地连接 属性”对话框

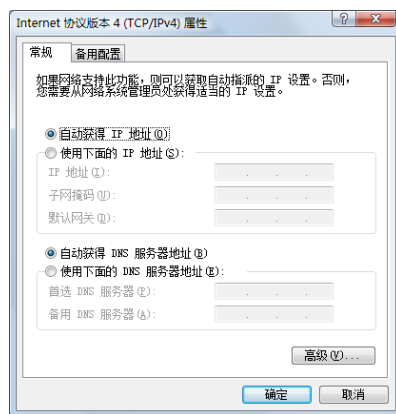


图 6-69 “Internet 协议版本 4 (TCP/IPv4) 属性”对话框

④ 单击“确定”按钮。

与 Windows XP 一样，Windows Vista 也可以在命令提示符中使用 IPConfig 命令来查看、释放并重新获取 IP 地址。

第 7 章 配置与管理打印服务

打印机是单位的常用设备，主要用来打印各种文档。虽然打印机的价格不高，但限于成本和空间，仍不会为每个用户都配备一台打印机，移动用户更不可能随身携带打印机。为了使所有用户都能打印，可利用网络打印来解决。不论直接连接到打印服务器，还是从其他位置接入网络的打印机都可以通过打印服务器统一管理，并为所有用户或指定用户完成打印任务。这样不仅节约购买打印机的费用，还能有效地控制打印成本。

7.1 安装打印机服务器

通过将打印机设置为网络共享，即可供网络中所有的用户使用，而不必为每台计算机都安装一台打印机。打印服务器可以管理网络中的多台打印机，并分别为不同的打印机分配不同的打印任务。

7.1.1 连接共享打印机

在网络中共享打印机时，主要有两种不同的连接模式，即“打印服务器+打印机”模式和“打印服务器+网络打印机”模式。

“打印服务器+打印机”模式将一台普通打印机安装在作为打印服务器上，然后通过网络共享该打印机，供局域网中的授权用户使用。打印服务器既可以由通用计算机承担，也可以由专门的打印服务器承担。如果网络规模比较小，则可以采用普通计算机，操作系统可以采用 Windows 2000/XP/Vista；如果网络规模较大，则应当采用专门的服务器。操作系统也应当采用 Windows Server 2003 或 Windows Server 2008，从而便于管理打印权限和打印队列，并适应繁重的打印任务。采用计算机作为打印服务器的网络拓扑结构如图 7-1 所示。

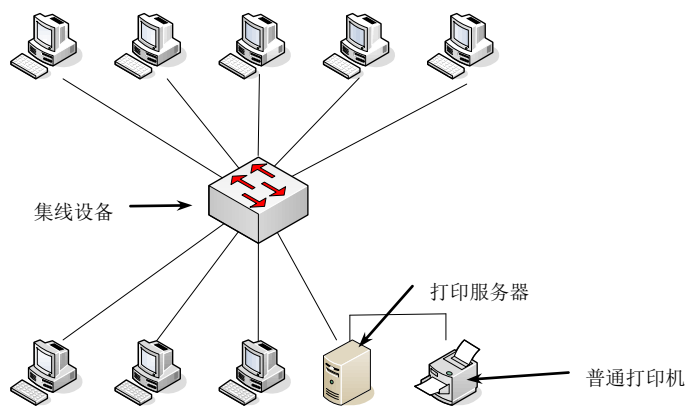


图 7-1 使用计算机作为打印服务器的网络拓扑结构

无论是针式打印机、喷墨打印机，还是激光打印机都可以充当共享打印机。由于喷墨打印机和激光打印机的打印速度快，并且可以批量放置纸张，所以在使用时更加方便。针式打印机由于无法自动进纸，因此最好选用连续纸。另外针式打印机的打印速度比较慢，打印精度也较差，所以除非是复写式打印；否则最好不要使用针式打印机。

“打印服务器+网络打印”模式是将一台带有网卡的网络打印机接入局域网，为其设置 IP 地址，使

其成为网络上的一个不依赖于其他计算机的独立节点。然后在打印服务器中管理该网络打印机，用户就可以用其打印。网络打印机模式的拓扑结构如图 7-2 所示，它通过 EIO 插槽直接连接网络适配卡，能够以网络的速度实现高速打印输出。

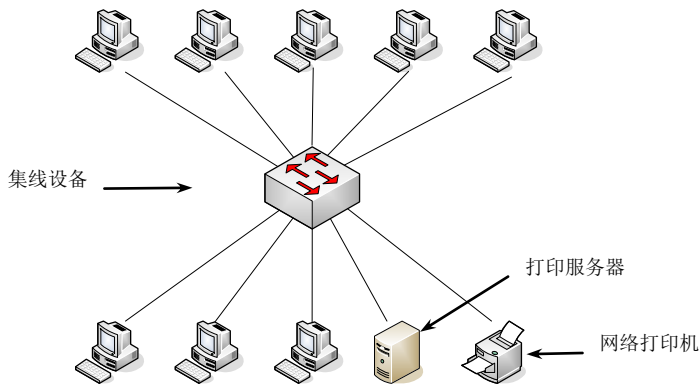


图 7-2 网络打印模式的拓扑结构

由于计算机的端口有限，因此使用普通打印机时打印服务器可管理的打印机数量也就较少。由于网络打印机采用以太网端口接入网络，一台打印服务器可以管理数量非常多的网络打印机，因此更适用于大型网络的打印服务。

7.1.2 安装打印服务器

为提供网络打印服务，必须首先将计算机安装为打印服务器。安装并设置共享打印机，然后为不同操作系统安装驱动程序，使得网络客户端在安装共享打印机时不再需要单独安装驱动程序。

① 运行“服务器角色添加向导”，在如图 7-3 所示的“选择服务器角色”对话框中选中“打印服务”复选框。

② 单击“下一步”按钮，显示如图 7-4 所示的“打印服务”对话框，其中显示打印服务简介和注意事项。

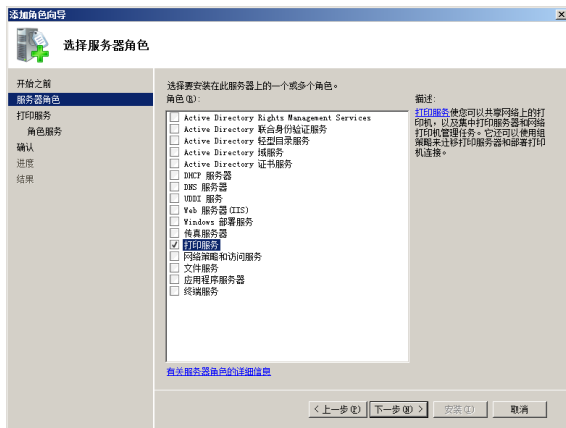


图 7-3 “选择服务器角色”对话框



图 7-4 “打印服务”对话框

③ 单击“下一步”按钮，显示如图 7-5 所示的“选择角色服务”对话框，选择为打印服务所安装的角色服务。“打印服务器”选项用于安装打印服务器，“LPD 服务”选项用于使基于 UNIX 的计算机或使用 Line Printer Remote (LPR) 服务的计算机可以使用该共享打印机，“Internet 打印”选项则使用户可以通过 Internet 使用和管理打印机。

④ 如果要使用 Internet 打印功能，则选中“Internet 打印”复选框，显示如图 7-6 所示的“是否添加 Internet 打印 所需的角色服务和功能”对话框。提示必须同时安装 IIS 服务和 Windows 进程

活服务，单击“添加必需的角色服务”按钮添加。

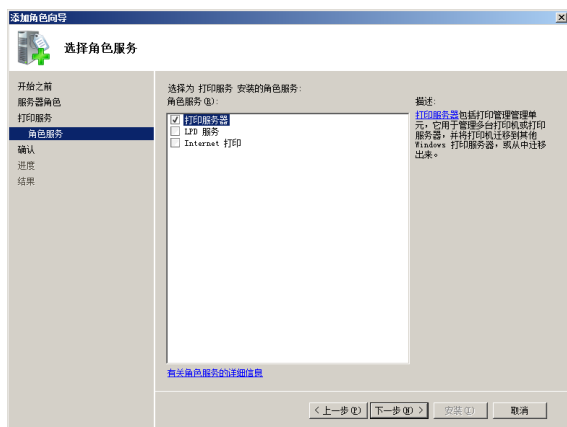


图 7-5 “选择角色服务”对话框

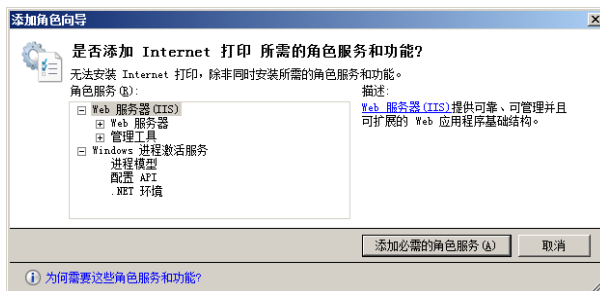


图 7-6 “是否添加 Internet 打印 所需的角色服务和功能”对话框

⑤ 单击“下一步”按钮，显示如图 7-7 所示的“Web 服务器 (IIS)”对话框，其中显示 Web 服务器的简介信息。

⑥ 单击“下一步”按钮，显示如图 7-8 所示的“选择角色服务”对话框。在其中选择待安装的 Web 服务器组件，一般使用默认设置即可。



图 7-7 “Web 服务器 (IIS)”对话框

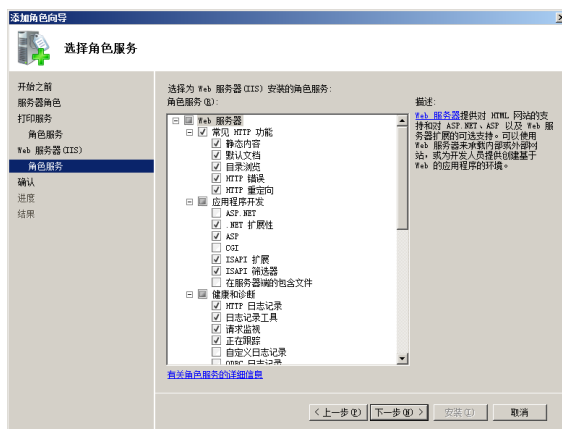


图 7-8 “选择角色服务”对话框

⑦ 单击“下一步”按钮，显示如图 7-9 所示的“确认安装选择”对话框，其中显示待安装的服务。如果需要更改，则单击“上一步”按钮返回。

⑧ 单击“安装”按钮开始安装打印服务，完成后显示如图 7-10 所示“安装结果”对话框。



图 7-9 “确认安装选择”对话框

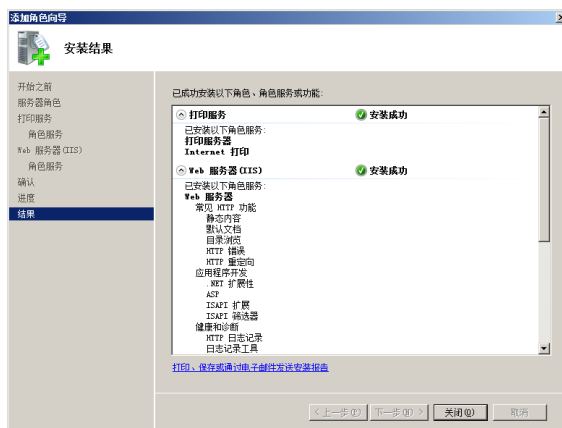


图 7-10 “安装结果”对话框

⑨ 单击“关闭”按钮完成打印服务器的安装，在如图 7-11 所示的“服务器管理器”窗口中依次展开“角色”→“打印服务”→“打印管理”选项，可添加和管理网络打印机。

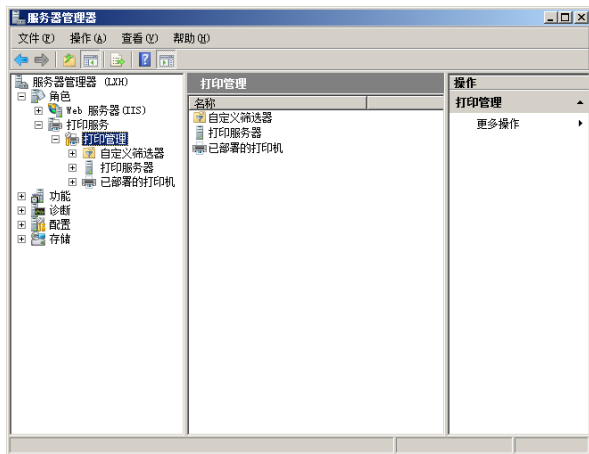


图 7-11 “服务器管理器”窗口

7.1.3 安装网络打印机

由于网络打印机直接连接到集线设备，而未连接到计算机的并行端口，因此一台打印机服务器可管理更多的打印机。网络接口打印机更适合于打印机数量较多的大中型网络，并且可以安装一台专门的打印服务器用于管理这些打印机。网络打印机可以在“控制面板”窗口中利用“添加打印机”向导添加。

- ① 单击“开始”→“控制面板”→“打印机”选项，打开“打印机”窗口，如图 7-12 所示。
- ② 双击“添加打印机”图标，运行“添加打印机”向导，显示如图 7-13 所示的“选择本地或网络打印机”对话框。

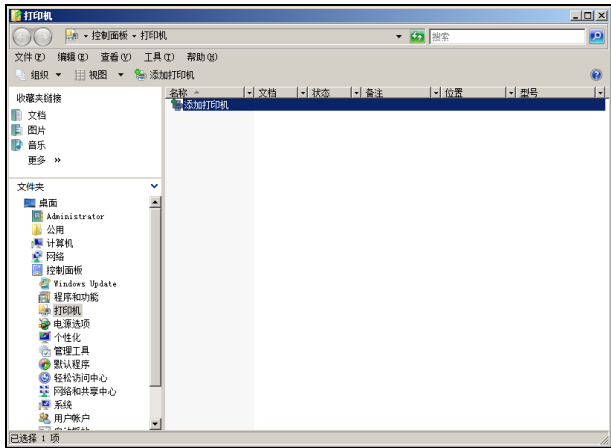


图 7-12 “打印机”窗口

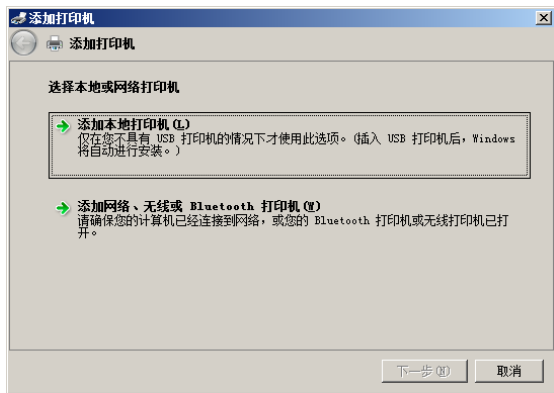


图 7-13 “选择本地或网络打印机”对话框

③ 单击“添加网络、无线或 Bluetooth 打印机”按钮，系统自动搜索网络中的共享打印机，如图 7-14 所示。

④ 如果没有搜索到网络打印机，则单击“我需要的打印机不在列表中”按钮，显示如图 7-15 所示的“按名称或 TCP/IP 地址查找打印机”对话框。选择“按名称选择共享打印机”单选按钮，并键入共享打印机的网络路径。

⑤ 单击“下一步”按钮，如果网络打印机设置了访问权限，则显示如图 7-16 所示的“正在连接到”对话框，键入用户名和密码即可。

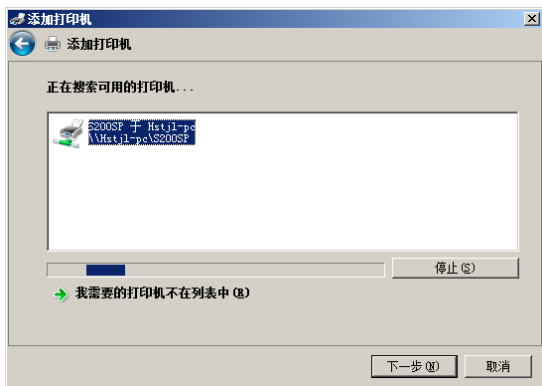


图 7-14 搜索网络中的共享打印机

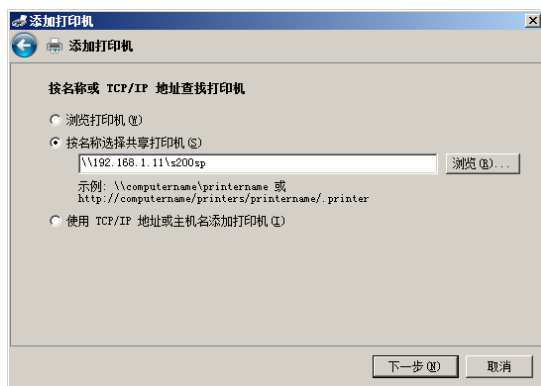


图 7-15 “按名称或 TCP/IP 地址查找打印机”对话框

⑥ 单击“确定”按钮，开始连接该打印机，连接成功后显示如图 7-17 所示的“键入打印机名称”对话框。选中“设置为默认打印机”复选框，可将该打印机设置为本地默认打印机。

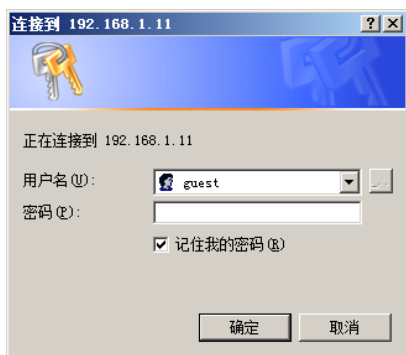


图 7-16 “正在连接到”对话框



图 7-17 “键入打印机名称”对话框

⑦ 单击“下一步”按钮，安装完成共享打印机，如图 7-18 所示。单击“打印测试页”按钮，可以测试所安装的打印机是否能够正常工作。

⑧ 单击“完成”按钮，安装的共享打印机显示在“打印机”窗口中，如图 7-19 所示。

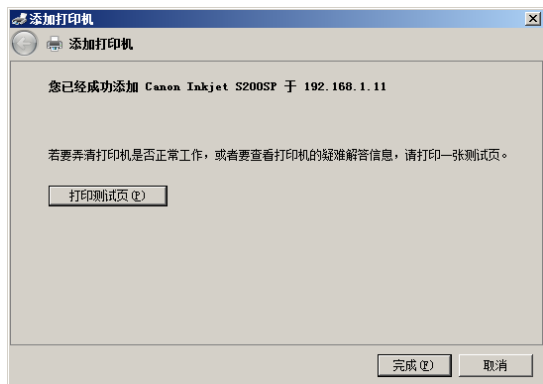


图 7-18 添加成功打印机

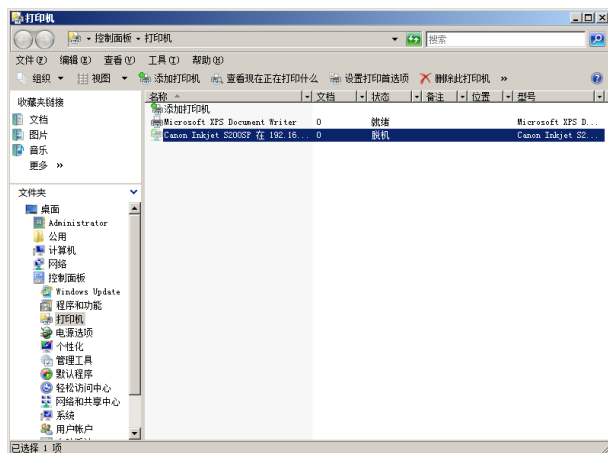


图 7-19 已安装的打印机

➤➤ 7.1.4 管理打印机驱动程序

打印机只有安装了相应的驱动程序才能用来打印，而不同版本的操作系统所使用的打印机驱动程序也不同。因此要根据网络中所使用的操作系统版本安装相应的驱动程序，使客户端可以自动从打印服务器下载安装。默认情况下，打印服务器会安装适合于 x86 计算机的 32 位驱动程序。

① 在“服务器管理器”窗口中依次展开“角色”→“打印服务器”→“打印管理”→“lzh(本地)”→“驱动程序”选项，显示如图 7-20 所示的“驱动程序”窗口，其中列出打印服务器中已安装的所有打印机。

② 右击“驱动程序”选项并选择快捷菜单中的“添加驱动程序”选项，打开“添加打印机驱动程序向导”对话框，如图 7-21 所示。

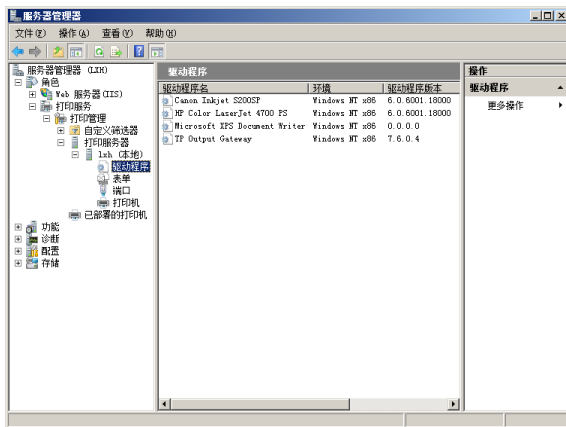


图 7-20 “驱动程序”窗口

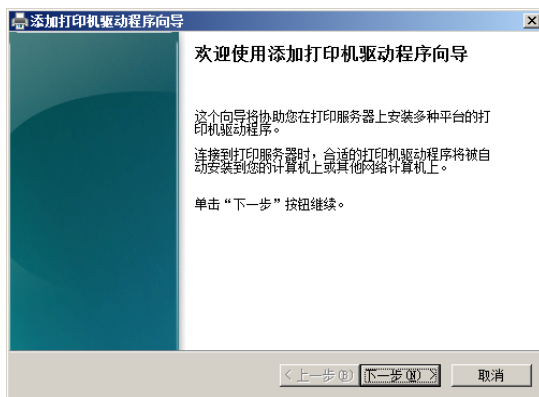


图 7-21 “添加打印机驱动程序向导”对话框

③ 单击“下一步”按钮，显示如图 7-22 所示的“处理器和操作系统选择”对话框，在列表框中选择待安装的驱动程序版本。

④ 单击“下一步”按钮，显示如图 7-23 所示的“打印驱动程序选项”对话框，选择待安装驱动程序的打印机型号。如果待安装的打印机型号没有显示在列表框中，则单击“从磁盘安装”按钮，并插入打印机驱动盘安装。

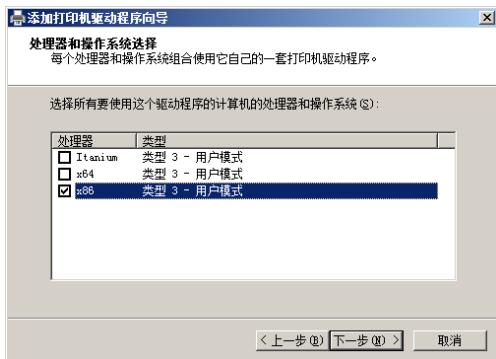


图 7-22 “处理器和操作系统选择”对话框

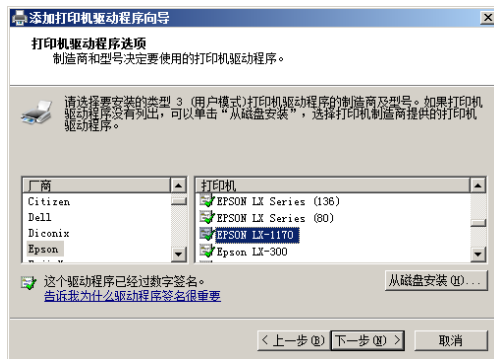


图 7-23 “打印驱动程序选项”对话框

⑤ 单击“下一步”按钮，显示如图 7-24 所示的“正在完成添加打印机驱动程序向导”对话框。

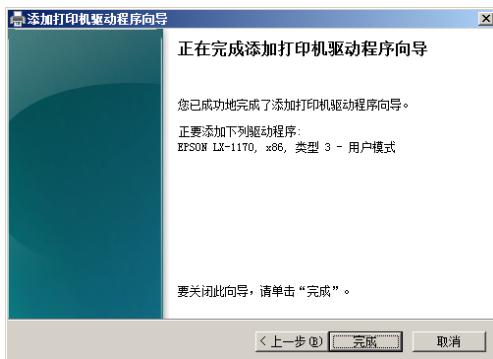


图 7-24 “正在完成添加打印机驱动程序向导”对话框

⑥ 单击“完成”按钮，安装成功打印机驱动程序并显示在“服务器管理器”窗口中。客户端在使用此种类型的打印机时，就会自动从打印服务器下载并安装相应的驱动程序。

7.1.5 迁移打印服务器

迁移打印服务器是从 Windows Vista 开始引入的功能，可通过运行“打印机迁移向导”或 `ptintbrm.exe` 命令导出打印队列、打印机设置、打印机端口和语言监视器等。然后导入到另一台 Windows 打印服务器上，从而可以合并打印服务器或者替换旧版打印服务器。

1. 导出打印服务器

① 在“服务器管理器”窗口中选择“打印管理”选项，右击并从快捷菜单中选择“迁移打印机”选项，运行“打印机迁移”向导。首先显示如图 7-25 所示的“打印机迁移”对话框，选择“将打印队列和打印机驱动程序导出到文件”单选按钮，可以将打印服务器数据备份到文件；选择“从文件中导入打印队列和打印机驱动程序”单选按钮，则将备份文件导入服务器。

② 单击“下一步”按钮，显示如图 7-26 所示的“选择打印服务器”对话框。选择“此打印服务器(\\lxh)”单选按钮，用来备份该打印服务器。如果要备份网络中的某台打印服务器，则选择“网络上的打印服务器”单选按钮。

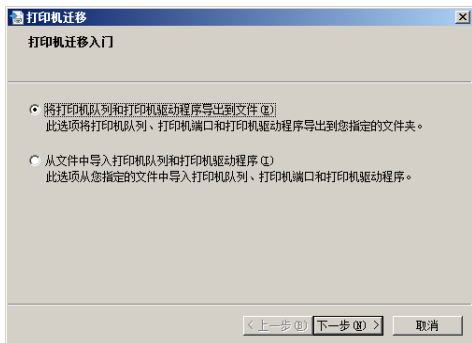


图 7-25 “打印机迁移入门”对话框

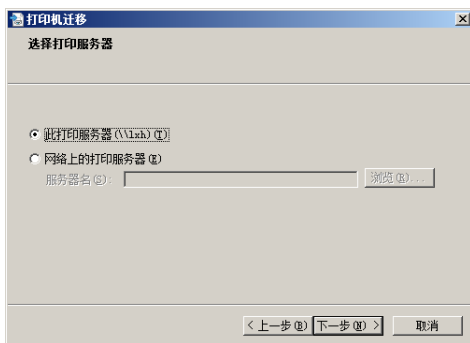


图 7-26 “选择打印服务器”对话框

③ 单击“下一步”按钮，显示如图 7-27 所示的“查看要导出的项目列表”对话框。其中列出要备份的内容，包括打印队列、打印机驱动程序和打印处理器等。

④ 单击“下一步”按钮，显示如图 7-28 所示的“选择文件位置”对话框。单击“浏览”按钮选择保存备份文件的路径，并设置一个名称，或者在“导出打印数据到”文本框中键入备份文件的路径和名称。



图 7-27 “查看要导出的项目列表”对话框

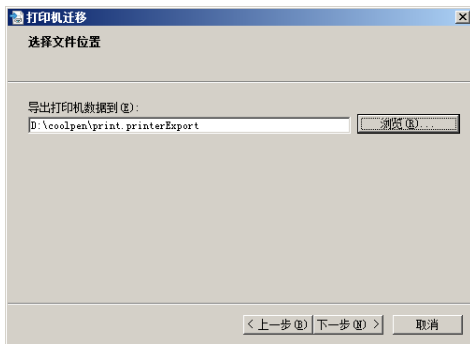


图 7-28 “选择文件位置”对话框

⑤ 单击“下一步”按钮导出打印服务器中的数据，完成后显示如图 7-29 所示的对话框，提示导出完成。

⑥ 单击“完成”按钮，备份完成打印服务器。

2. 导入打印服务器

① 在准备作为打印服务器的计算机中安装打印服务器，连接打印机，并将已备份的打印服务器数据文件复制到其中。

② 打开“服务器管理器”窗口，运行“打印机迁移向导”。在如图 7-30 所示的“打印机迁移入门”对话框中选择“从文件中导入打印机队列和打印机驱动程序”单选按钮，将备份文件导入到服务器。

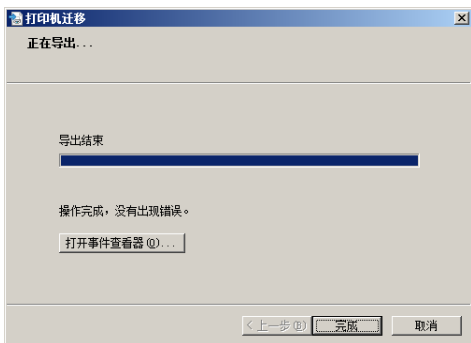


图 7-29 提示导出完成

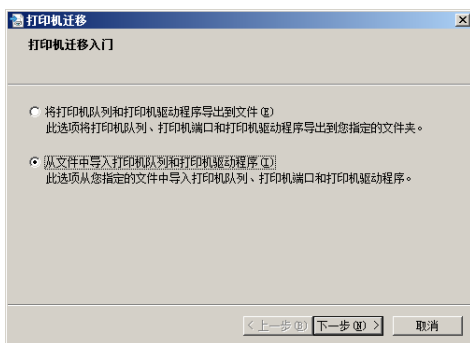


图 7-30 “打印机迁移入门”对话框

③ 单击“下一步”按钮，显示如图 7-31 所示的“选择文件位置”对话框。单击“浏览”按钮，选择打印服务器的备份文件。

④ 单击“下一步”按钮，显示如图 7-32 所示的“查看导入的项目列表”对话框，其中显示该备份文件中所包含的内容。

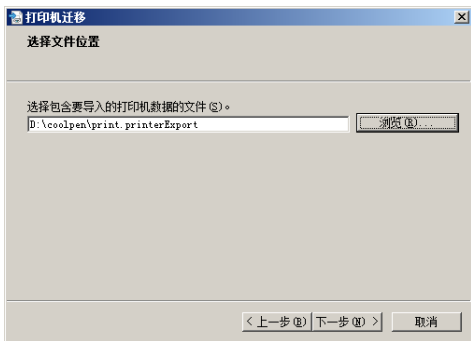


图 7-31 “选择文件位置”对话框



图 7-32 “查看导入的项目列表”对话框

⑤ 单击“下一步”按钮，显示如图 7-33 所示的“选择打印服务器”对话框，根据需要设置将该备份文件导入到的服务器。

⑥ 单击“下一步”按钮，显示如图 7-34 所示的“选择导入选项”对话框。在“导入模式”下拉列表框中选择“覆盖现有打印机”或者“保留现在打印机；导入副本”选项。

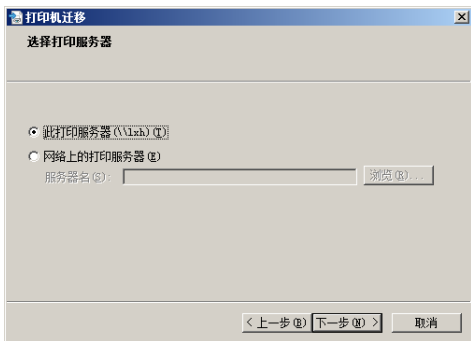


图 7-33 “选择打印服务器”对话框

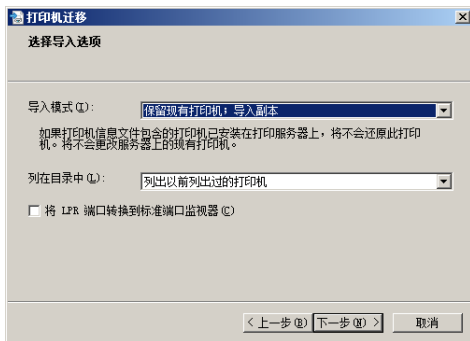


图 7-34 “选择导入选项”对话框

⑦ 单击“下一步”按钮开始导入，完成后显示如图 7-35 所示的对话框，提示导入完成后单击“完成”按钮完成备份文件的导入。

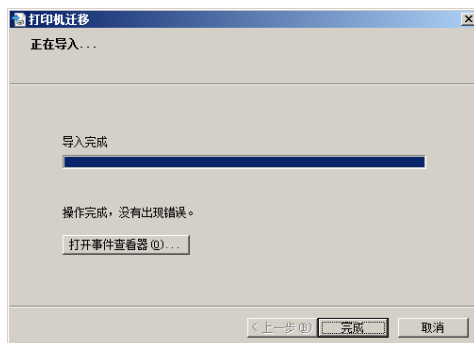


图 7-35 提示导入完成

7.2 管理打印服务器

由于网络中需要打印的文档比较多，因此需要调度管理打印服务器，例如为不同的打印机分配打印任务、调整打印任务及管理打印文档等。同时，还可以为不同的用户设置不同的打印权限来限制访问打印机。

7.2.1 管理打印队列

打印队列用来存放等待打印的文档，当用户在应用程序中选择了“打印”命令后，Windows 就会创建一个打印任务。如果打印机此时正在处理另一项打印任务，则在打印机文件夹中形成一个打印队列，保存所有等待打印的文档。

1. 调整打印文档

打印机的打印队列中可能会有多个等待打印的文档，为了提高打印效率，网络管理员应当查看打印队列中的打印文档。并且更改打印优先级来调整打印文档的打印次序，使急需的重要文档优先打印。

(1) 在“服务器管理器”窗口中打开“打印管理”控制台，展开“打印机”窗口。选择待查看的打印机，右击并从快捷菜单中选择“打开打印机队列”选项。显示如图 7-36 所示的打印队列，其中列出所有要打印的文档。

(2) 选择要调整打印次序的文档，右击并从快捷菜单中选择“属性”选项，显示如图 7-37 所示的文档属性。

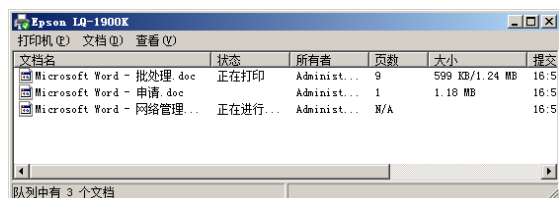


图 7-36 打印队列

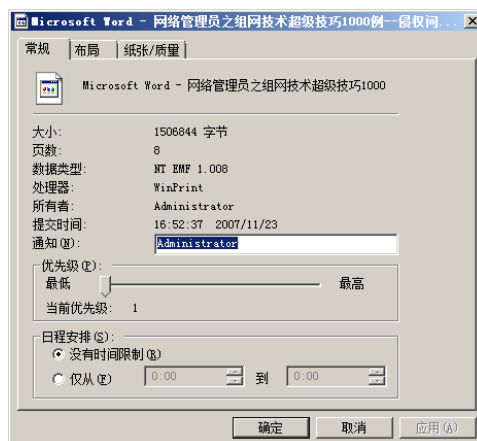


图 7-37 文档属性

(3) 在“优先级”选项组中拖动滑块即可改变所选文档的优先级。对于需要提前打印的文档,提高其优先级;对于不需要提前打印的文档,降低其优先级。

(4) 单击“确定”按钮,保存所做设置。

提示

当某一文档正在打印时,不能调整其优先级。

2. 暂停和继续打印一个文档

如果用户需要暂时停止打印某个文档,可在打印队列中将该文档“暂停打印”,优先打印其他文档。当需要继续打印时,只需在打印文档的快捷菜单中选择“继续”选项即可。

在打印队列窗口中,右击要暂停打印的文档。从快捷菜单中选择“暂停”选项,即可暂停打印该文档。同时“状态”栏中显示“已暂停”字样,如图 7-38 所示。

如果某个文档需要取消打印,可以将其在打印队列中删除。选择要取消打印的文档,右击并选择快捷菜单中的“取消”选项,将文档删除即可。如果需要清除所有的打印文档,则在打印队列窗口中单击“打印机”→“取消所有文档”选项。

3. 暂停和重新启动打印机的打印作业

打印机需要不定时维护,例如添加打印纸、更换硒鼓或色带等打印材料等。此时就需要管理员暂停打印工作,当维护完成后继续打印工作。

① 在“服务器管理器”窗口中打开“打印管理”控制台,选择待暂停打印的打印机。右击并选择快捷菜单中的“暂停打印”选项,即可使打印机暂停工作。此时该打印机的“队列状态”中显示为“已暂停”,如图 7-39 所示。



图 7-38 暂停打印文档

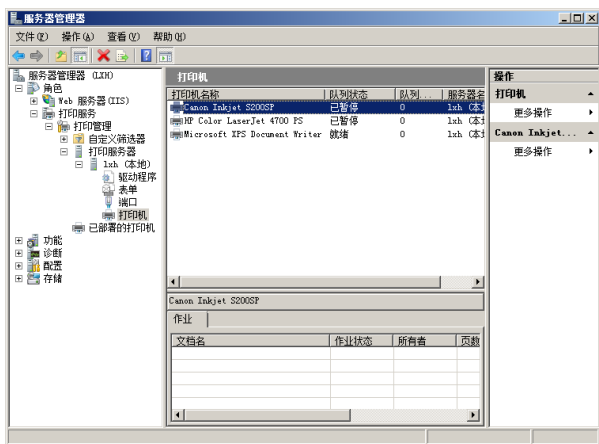


图 7-39 暂停打印机

② 当需要重新启动打印机打印工作时,右击已暂停的打印机。选择快捷菜单中的“恢复打印”选项即可使打印机继续打印,同时“队列状态”中的“已暂停”变为“就绪”。

7.2.2 创建打印池

打印池是一台逻辑打印机,在其中可以添加并管理打印服务器上的多台打印机,将接收到的打印文档分配给其他空闲的打印机。用户在打印文档时,不再需要查找哪一台打印机目前可用。逻辑打印机将自动检查可用的端口,并按端口的添加顺序将文档发送到各个端口,从而减少了用户的等待时间。

创建打印池的操作步骤如下。

① 在“服务器管理器”的“打印管理”窗口中选择“打印管理”选项,选择待创建打印池的打印机。右击并选择快捷菜单中的“属性”选项,显示如图 7-40 所示的打印机属性对话框。

② 打开如图 7-41 所示的“端口”选项卡,在端口列表中选择打印机池连接的每台打印机的端口,

选中“启用打印机池”复选框。

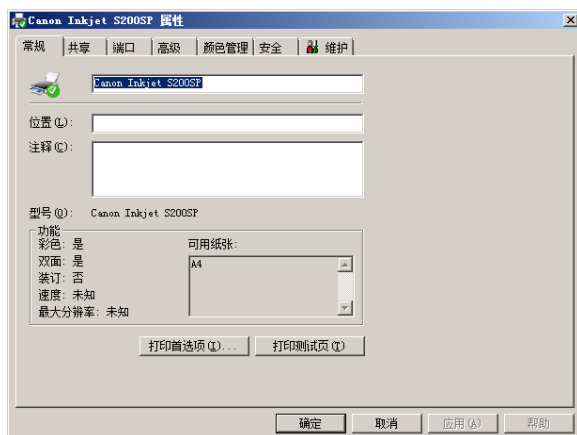


图 7-40 打印机属性对话框

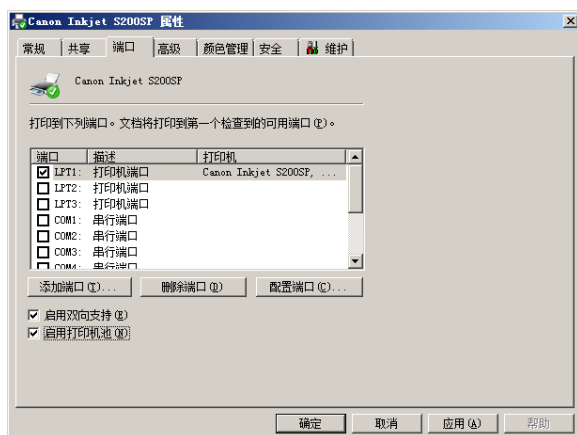


图 7-41 “端口”选项卡

提示 必须选择一个以上的端口；否则在单击“确定”按钮后将显示如图 7-42 所示的警告框，提示如果少于两个端口，则打印池无法使用。

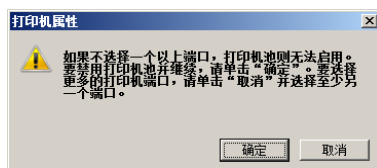


图 7-42 警告框

③ 单击“确定”按钮，保存所做设置即可。

注意

在设置打印池之前，池中的所有打印机必须使用同样的驱动程序。由于用户不知道发出的文档由池中的哪一台打印机打印，因此应将池中的所有打印机放置在同一地点。

7.2.3 设置打印机权限

安装打印机以后，默认允许所有用户打印，并允许选择用户或组管理打印机或发送给它的文档。为了合理安排打印机的使用，可以通过为用户指派打印机权限来控制。例如，可以为部门中所有无管理权用户设置“打印”权限，而为所有管理人员设置“打印和管理文档”权限。这样所有用户和管理人员都能打印文档，但管理人员还能更改发送给打印机的任何文档的打印状态。

1. 为不同用户设置不同的打印权限

① 在打印机属性对话框中打开“安全”选项卡，如图 7-43 所示。在“组或用户名”文本框中选择一个用户，即可在权限列表框中为该用户选择权限。

Windows 提供了 4 种打印安全权限，即打印、管理打印机、管理文档和特殊权限。当为一组用户指派了多个权限时，将应用限制性最少的权限。但是应用了“拒绝”权限时，则其优先于其他任何权限。4 种权限及其意义如下。

- 打印：用户可以连接的打印机，并将文档发送到打印机。默认情况下，Everyone 组具有此权限。
- 管理打印机权限：用户可以执行与“打印”权限相关联的任务，并且具有对打印机的完全管理控制权。例如暂停和重新启动打印机、更改打印后台处理程序设置、共享打印机、调整打印机权限等，还可以更改打印机属性。默认情况下，Administrators 和 Power Users 组具有此

权限。

- 管理文档权限：用户可以暂停、继续、重新开始和取消打印队列的文档，并可重新安排文档顺序，但无法将文档发送到打印机或控制打印机状态。默认情况下，Creator Owner 组具有此权限。
- 拒绝：相应的权限选中该复选项后为拒绝。

② 如果要为新用户账户设置权限，单击“添加”按钮，显示如图 7-44 所示的“选择用户或组”对话框，在“输入对象名称来选择”文本框中键入要为其设置权限的用户或组名称。

③ 依次单击“确定”按钮保存所做设置。

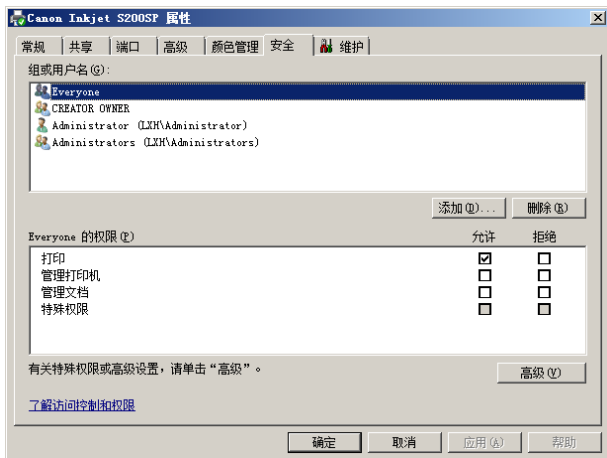


图 7-43 “安全”选项卡

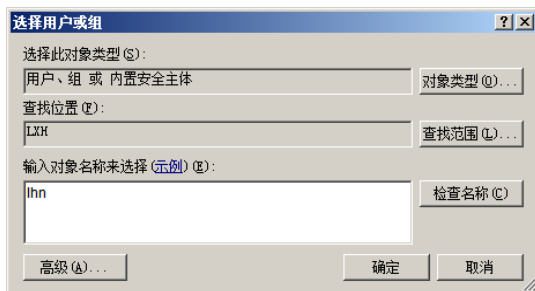


图 7-44 选择用户或组

2. 设置打印机的所有者

默认情况下，打印机的所有者是安装打印机的用户。如果该用户不再能够管理这台打印机，则应当将管理这台打印机的权限转移给其他用户。能够成为打印机的所有者的用户或组如下。

- (1) 由管理员定义的具有管理打印机权限的用户或组成员。
- (2) 系统提供的 Administrators、Print Operators、Server Operators，以及 Power User 组的成员。

如果要成为打印机的所有者，首先要使用户具有管理打印机的权限，或者加入上述组成为其成员。设置为打印机所有者的操作步骤如下。

① 在打印机属性对话框中打开“安全”选项卡。单击“高级”按钮，显示如图 7-45 所示的高级安全设置对话框。



图 7-45 高级安全设置对话框



② 打开“所有者”选项卡，如图 7-46 所示，在“当前所有者”文本框中显示当前成为打印机所有者的组，如果需要更改打印机所有者组或用户，则在“将所有者更改为”列表框中选择需要设置打印机所有者的组或用户。如果其中没有所需用户或组，则单击“其他用户或组”按钮选择。

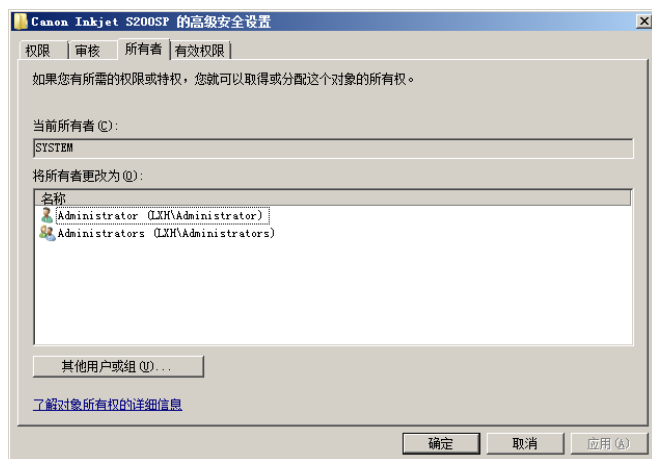


图 7-46 “所有者”选项卡

③ 单击“确定”按钮保存所做设置。



注意：

打印机的所有权不能从一个用户指定到另一个用户，只有当原先具有所有权的用户无效时才能指定其他用户，只有 Administrator 可以把所有权指定给 Administrators 组。



7.2.4 利用分隔页分隔打印文档

由于网络打印机可供多人同时使用，因此一台打印机中可能已经有多份打印的文档，很难区分文档所属的用户。可以利用分隔页分隔每份文档，即在打印每份文档之前首先打印该分隔页的内容，其中可以包含拥有该文档的用户名称、打印日期及打印时间等说明。分隔页文档除了可供打印分隔页之外，还具有控制打印机工作的功能。

1. 创建分隔页文档

在 Windows Server 2008 系统内置了如下多个标准分隔页文档，位于 C:\Windows\system32 文件夹中。

(1) SYSPRINT.SEP：适用于与 PortScript 兼容的打印设备。

(2) PCL.SEP：适用于与 PCL 兼容的打印设备，它将打印设备切换到 PCL 模式，然后打印分隔页。

(3) PSCRIPT.SEP：适用于与 PortScript 兼容的打印设备，用来将打印设备切换到 PostScript 模式，但是不会打印分隔页。

(4) SYSPRTJ.SEP：为日本版。

如果以上标准的分隔页文件不符合用户要求，则可以使用“记事本”自行设置。

2. 选择分隔页文档

① 在打印机属性对话框中打开“高级”选项卡，如图 7-47 所示。

② 单击“分隔页”按钮，显示如图 7-48 所示“分隔页”对话框。在“分隔页”文本框中键入分隔页的路径及文件名，或者单击“浏览”按钮选择。

③ 单击“确定”按钮保存设置。

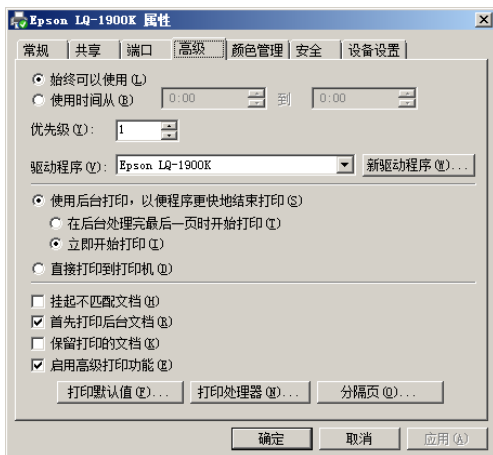


图 7-47 “高级”选项卡

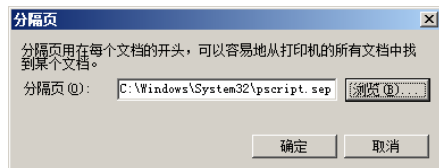


图 7-48 选择分隔页文档

7.2.5 设置送纸器

有的打印机有多个送纸器，可以分别放置有不同的纸张，例如 A4 及 B5 等。为了便于用户使用，可为送纸器指定所使用的纸张。用户在打印时，只要选择打印纸张即可。无需知道纸张放在哪个送纸器内，打印机会自动从纸张所在的送纸器内取纸。

在打印机属性对话框中打开“设备设置”选项卡，即可根据实际需要指定送纸器内的纸张，如图 7-49 所示。

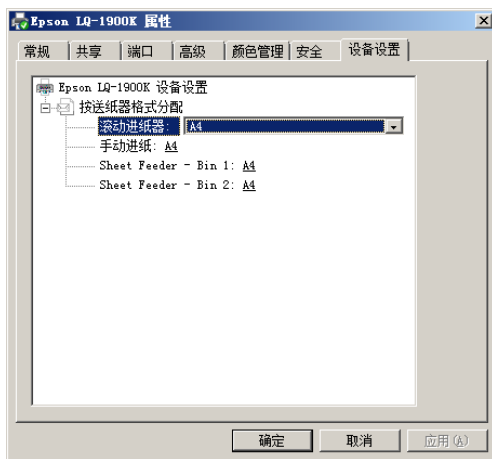


图 7-49 指定送纸器内的纸张

设置后单击“确定”按钮。

7.2.6 管理等待打印的文档

当打印服务器收到打印文档后，这些文档会在打印机内排队等待打印。如果用户具备管理打印机的权限，则可以针对这些文档执行管理任务，如暂停、继续、重新开始及取消打印等。

1. 暂停、继续、重新开始及取消打印文档

如果有些文档在打印时出现问题，则可以暂停打印，待解决问题后重新或者取消打印。

在“打印管理”控制台中右击打印机，选择快捷菜单中的“打开打印队列”选项，显示的打印队列如图 7-50 所示。

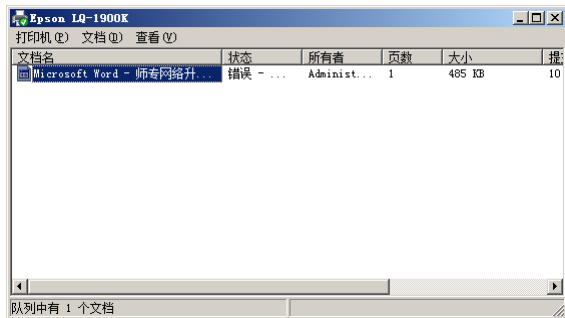


图 7-50 打印队列

选择要处理的文件，打开“文档”菜单即可处理该打印文档，其中包括如下选项。

- (1) 暂停：暂停打印该文档。
- (2) 继续：继续打印被暂停的文档。
- (3) 重新启动：从第 1 页开始重新打印。
- (4) 取消：取消打印该份文档。

2. 暂停或取消打印所有文档

如果打印机出现问题，则可以暂停打印所有的文档，待解决问题后重新打印或者取消打印。打开打印队列窗口中的“打印机”菜单，可选择如下选项处理所有文档。

- (1) 暂停打印：暂停打印所有的文档，清除后会继续打印。
- (2) 取消所有文档：取消打印所有在该打印机排队等待打印的文档，并在队列中删除这些文档。

3. 设置通知人、优先级与打印时间

用户可以针对正在等待打印的文档设置其打印完成后的通知人、打印优先级与打印时间。

在“打印机”窗口中双击打印机图标，右击要打印的文档。选择快捷菜单中的“属性”选项，显示如图 7-51 所示文档属性对话框。

在其中可以设置如下选项。

- (1) 通知：设置当文档打印完成时通知打印作者，以便使其知道自己的文档已经打印完成，也可改变通知人。
- (2) 优先级：同一个打印机内文档的打印优先级是相同的，但通过拖动滑块可以改变该文档的打印优先级，以便让该文档优先打印。
- (3) 日程安排：更改该文档的打印时间，在时间未到之前，该文档不会被打印。

4. 重定向打印文档

如果因打印机出现故障，造成正在打印机内排队等待打印的文档无法从该打印机打印时，可以将这些文档转到其他打印机继续打印。不过，所转移的打印机必须安装了相同的打印机驱动程序，即打印机是相同或兼容的。

- (1) 在“打印管理”控制台中，选择要被重定向的打印机。右击并选择快捷菜单中的“属性”选项，打开打印机属性对话框。打开“端口”选项卡，如图 7-52 所示。
- (2) 在列表框中选择待重定向到的打印机，单击“确定”按钮即可。



注意：

在重定向时除了正在打印的文档，其他所有等待打印的文档都会被重定向，但用户无法重定向某个文档。



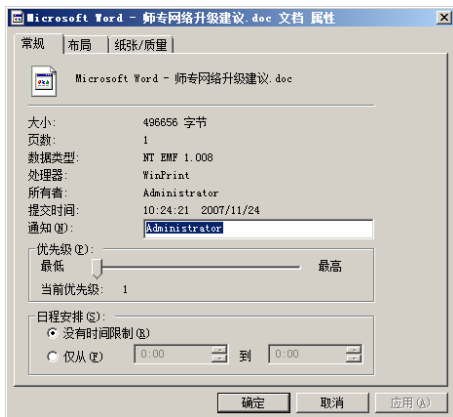


图 7-51 文档属性对话框

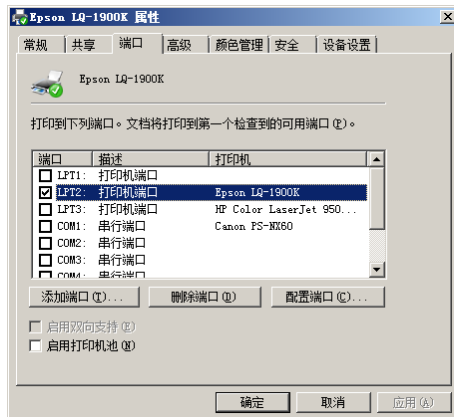


图 7-52 “端口”选项卡

7.3 共享网络打印机

打印服务器设置成功以后，即可在客户端安装共享打印机并用来打印文档。而客户端在安装网络打印机时，无需专门提供打印机驱动程序，系统会自动从打印服务器下载相应的驱动程序。如果某台计算机连接打印机，也可以将该打印机共享，供网络中的其他客户端使用。

7.3.1 安装打印机客户端

在客户端安装网络打印机时，可以在“控制面板”窗口通过“添加打印机”向导完成。不同操作系统中添加网络打印机的方式略有不同，这里以 Windows Vista 为例。

- ① 在“控制面板”窗口中打开“打印机”窗口，如图 7-53 所示。
- ② 单击标题栏中的“添加打印机”按钮，打开“添加打印机”对话框，如图 7-54 所示。

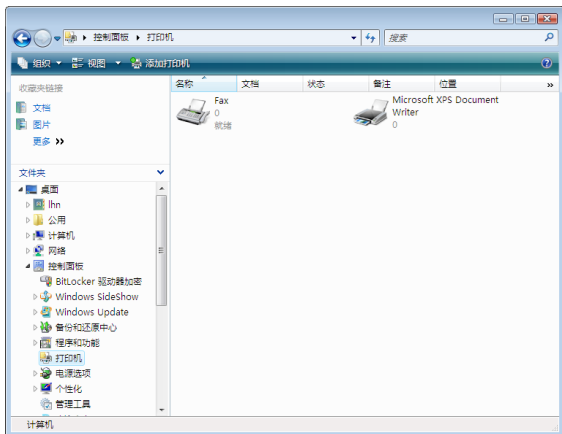


图 7-53 “打印机”窗口

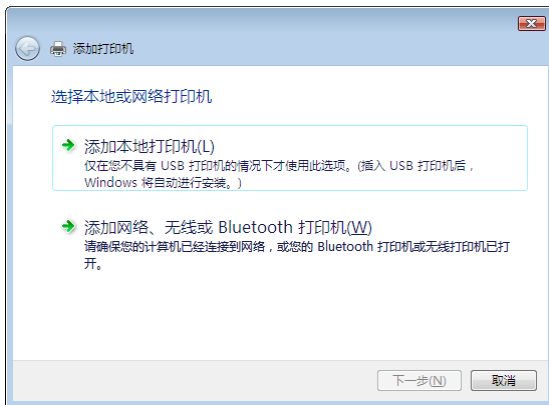


图 7-54 “添加打印机”对话框

③ 单击“添加网络、无线或 Bluetooth 打印机”按钮，系统开始搜索局域网中的共享打印机并将搜索到的打印机显示在“正在搜索可用的打印机”对话框中，如图 7-55 所示。

④ 选择待安装的共享打印机，单击“下一步”按钮开始连接该打印机（如图 7-56 所示），连接成功后即可添加。

⑤ 如果系统没有搜索到需要添加的打印机，则在“正在搜索可用的打印机”对话框中单击“我需要的打印机不在列表中”按钮，显示如图 7-57 所示的“按名称或 TCP/IP 地址查找打印机”对话框。选择“按名称选择共享打印机”单选按钮，并键入共享打印机的网络路径和名称，其格式为

\\打印服务器名称或 IP 地址\打印机共享名

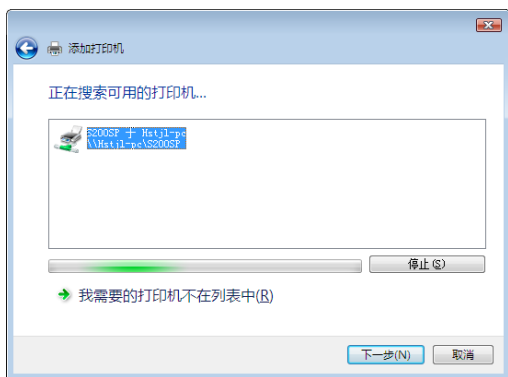


图 7-55 “正在搜索可用的打印机”对话框

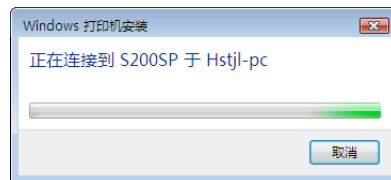


图 7-56 连接网络打印机

⑥ 单击“下一步”按钮，开始连接该打印机，连接成功后显示如图 7-58 所示的“键入打印机名称”对话框。如果选中“设置为默认打印机”复选框，可将该打印机设置为默认打印机；否则清除该复选框。

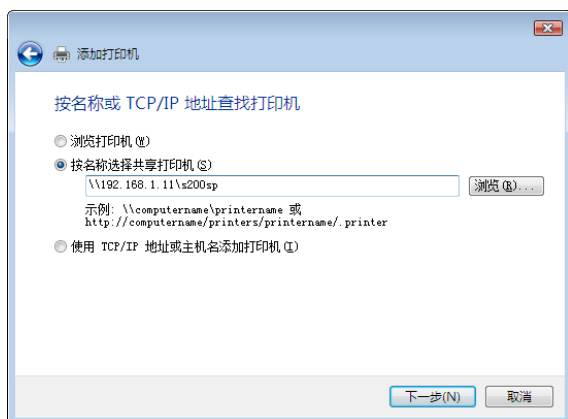


图 7-57 “按名称或 TCP/IP 地址查找打印机”对话框

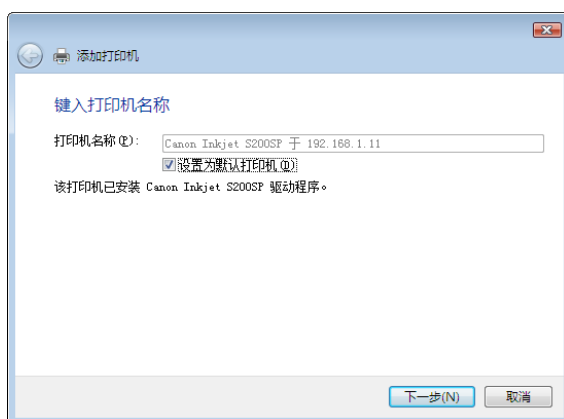


图 7-58 “键入打印机名称”对话框

⑦ 单击“下一步”按钮，提示打印机已添加成功，如图 7-59 所示。

⑧ 单击“完成”按钮，共享打印机安装成功并显示在“打印机”窗口中，如图 7-60 所示。

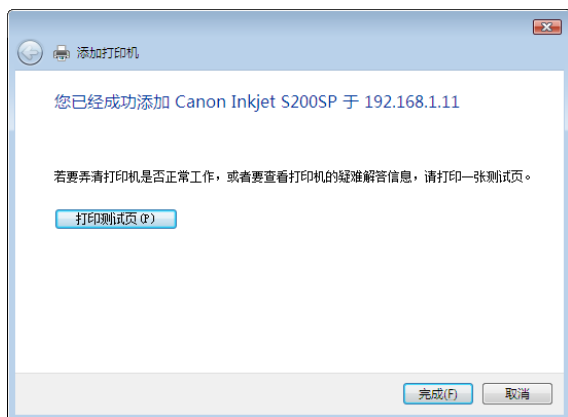


图 7-59 打印机添加成功

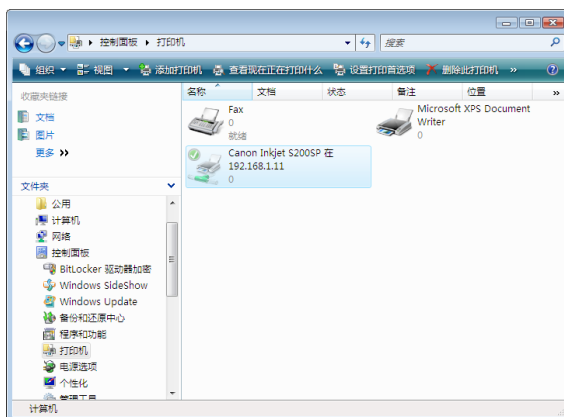


图 7-60 添加的打印机

7.3.2 安装 Web 共享打印机

如果打印服务器中安装了“Internet 打印”功能，那么用户可以借助 Web 浏览器，通过 Internet 远程连接到打印服务器并使用网络打印机打印。由于 Web 方式不受路由限制，所以可以使处于不同网

段的用户使用网络打印机。

通过“控制面板”窗口运行“添加打印机”向导，在如图 7-61 所示的“按名称或 TCP/IP 地址查找打印机”对话框中选择“按名称选择共享打印机”单选按钮，并键入 Web 共享打印机路径，格式如下：

http://打印服务器的 IP 地址或 DNS 名称/printers/打印机共享名/.printer

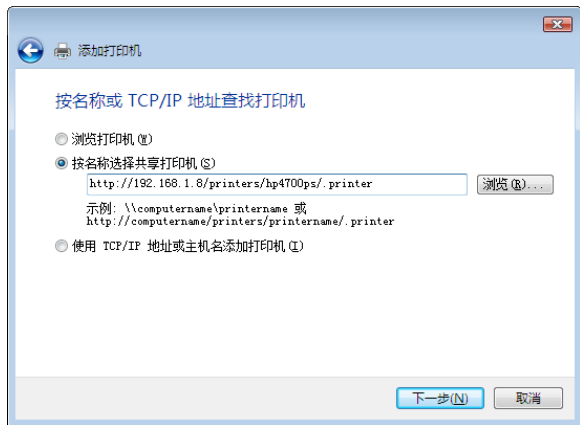


图 7-61 “按名称或 TCP/IP 地址查找打印机”对话框

单击“下一步”按钮添加该打印机。

7.3.3 使用浏览器连接到打印机

使用浏览器连接到打印机的操作步骤如下。

① 打开 Web 浏览器，在地址栏中键入打印服务器的 Web 地址，格式为：

http://打印服务器的 IP 地址或 DNS 名称/printers

② 按回车键，显示如图 7-62 所示的“连接到...”对话框，提示需要登录。

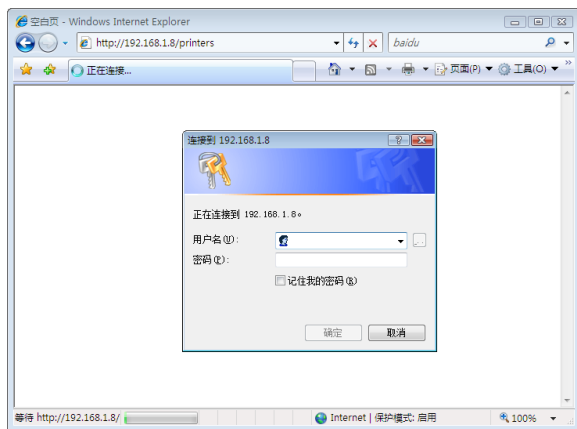


图 7-62 “连接到...”对话框

③ 输入具有访问权限的用户账户名和密码登录，单击“确定”按钮连接打印服务器。显示打印服务器上的打印机，如图 7-63 所示。

④ 单击打印机名称，显示打印机上的打印文档。由于需要安装 ActiveX 控件，因此会在窗口上方显示信息栏。右击该信息栏并选择快捷菜单中的“安装 ActiveX 控件”选项，显示如图 7-64 所示的“安全警告”对话框。

⑤ 单击“运行”按钮，安装该 ActiveX 控件。此时可查看这台打印机的打印队列，如图 7-65 所示。

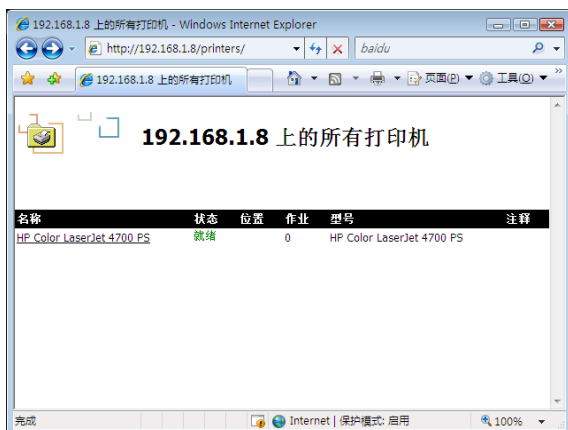


图 7-63 打印服务器上的打印机

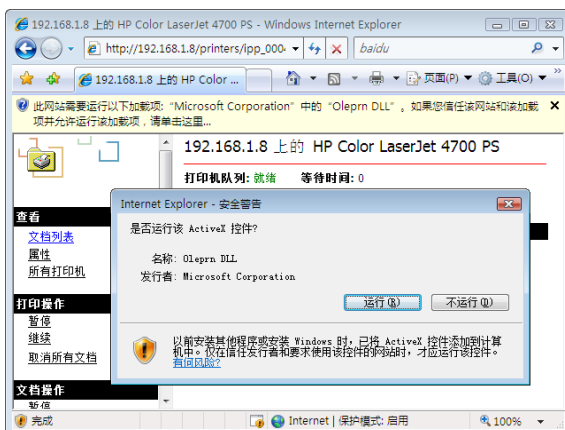


图 7-64 “安全警告”对话框

在其中可查看所有的打印机、打印文档，以及打印机属性等（如图 7-66 所示），还可控制打印任务，如暂停、继续及取消打印文档等。

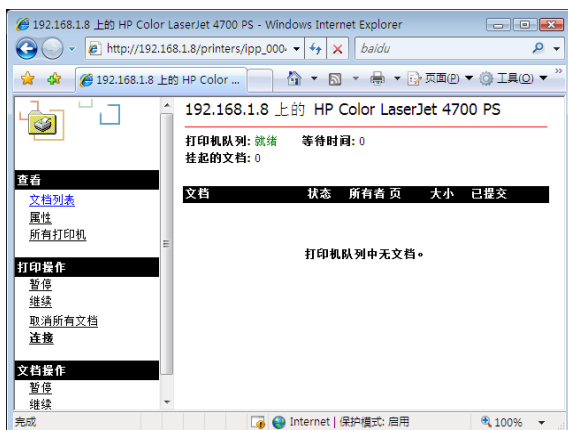


图 7-65 打印队列

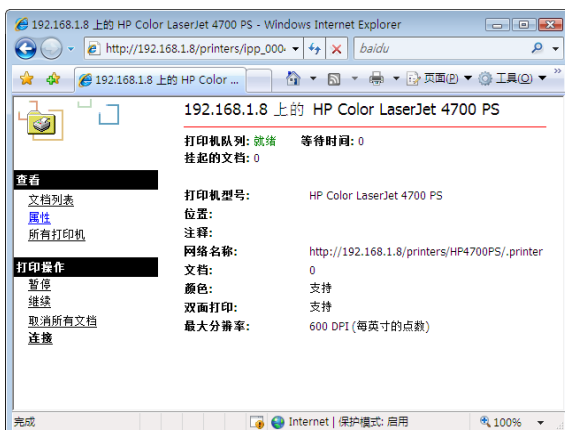


图 7-66 打印机属性

7.3.4 使用“网上邻居”安装打印机

除了可以采用“打印机安装向导”安装网络打印机外，还可以使用“网上邻居”方式安装。

① 通过“网上邻居”搜索找到打印服务器，列出其中的所有共享文件夹及共享打印机，如图 7-67 所示。

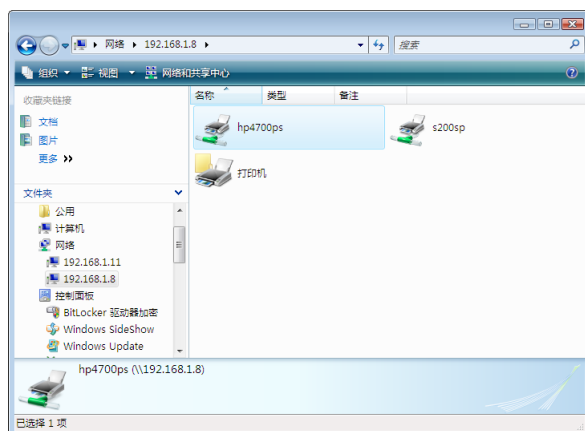


图 7-67 打印服务器的所有共享文件夹及共享打印机

② 双击待安装的打印机名称，显示如图 7-68 所示的警告框，提示要使用该共享打印机必须安装该打印机的驱动程序。

③ 单击“是”按钮，安装驱动程序，安装完成后会显示如图 7-69 所示的打印任务窗口。同时将该打印机添加到“控制面板”的“打印机”窗口中。

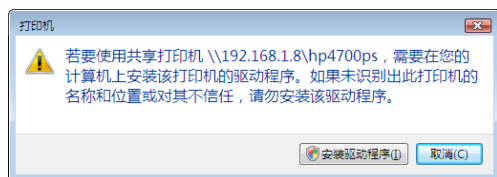


图 7-68 警告框

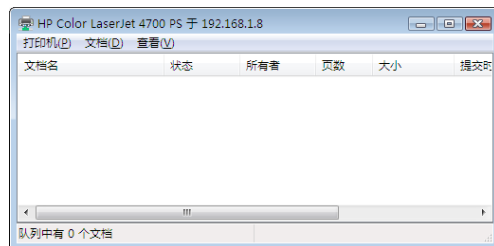


图 7-69 打印任务窗口

第 8 章 配置与管理 Web 服务

Web 服务是网络中应用最广泛的服务，主要用来搭建 Web 网站发布公司信息、宣传产品，甚至实现网上交易及信息反馈等。虽然很多企业都提供网站空间租用，但价格不菲。Windows Server 2008 内置了功能强大的 Web 服务功能，可以搭建功能完备的 Web 网站，支持 ASP 和 .NET 动态功能。并且支持使用 Apache 等应用程序搭建各种动态网站，既节约资金，又便于管理。

8.1 IIS 概述

IIS (Internet Information Services, Internet 信息服务管理器) 是一个用于配置应用程序池或网站、FTP 站点、SMTP 或 NNTP 站点且基于 MMC 控制台管理程序，它是 Windows Server 2003/2008 操作系统自带的组件，无须安装第三方程序即可用来搭建各种网站并管理服务器中的所有站点。

8.1.1 IIS 简介

IIS 集成于 Windows Server 操作系统中，在 Windows Server 2008 系统中的 IIS 版本为 7.0。IIS 服务可以管理 Web 应用程序和 XML Web 服务，并用来搭建 Web 网站，同时为 Intranet 和 Internet 提供信息发布功能。它全面支持 ASP 和 .NET，可以运行当前流行且具有动态交互功能的 ASP 网页，并支持开发人员使用任何与 .NET 兼容的语言（包括 Visual Basic .NET、C# 和 Jscript .NET）编写 Web 应用程序。

IIS 服务可通过 IIS 管理器管理，这是一个综合性的 Internet 信息服务器。不仅提供了 WWW 服务、FTP 服务、SMTP 服务、NNTP 服务及 IIS 管理服务，还可以实现信息发布、文件传输及用户通信，并管理这些服务。

8.1.2 IIS 7.0

Windows Server 2008 中的 IIS 7.0 与以前的 IIS 服务有本质的区别，它完全以“按需定制”的模式展现，管理员可以只安装所需要的组件。由于安装组件的减少，被攻击面也随之降低，安全性也越来越高。同时，IIS 7.0 管理界面比以前的版本更加友好。

1. 组件化定制

IIS 7.0 被分割成 40 多个不同功能的模块，例如身份验证、静态页面、IIS 管理器授权及 ASP.NET 等。网络管理员可根据需要定制安装相应的功能模块，不需要的模块将不会被加载到内存。这样使得 Web 网站的受攻击面减小，安全性和性能大大提高并且更易于管理，如图 8-1 所示。

2. XML 配置和部署

IIS 7.0 的配置工作可以完全通过 XML 文件来实现，管理工具使用了新的分布式 web.config 配置模式。它不再使用 metabase 配置存储，而使用和 ASP.NET 同样的 web.config 文件模型，允许用户把配置和 Web 应用内容一起存储和部署。管理员只需借助 Xcopy 工具，将现行配置文件复制到新服务器上即可，不需再重新编写管理脚本来定制配置。在新的 IIS 7.0 中，所有配置都存储在“.config”文件中，其所使用的格式为 XML，文件的保存位置为 C:\Windows\System32\inetsrv\config 目录下的 ApplicationHost.config 文件。其中保存了 IIS 的一些基本设置和策略，以及一些安装设置，如图 8-2 所示。

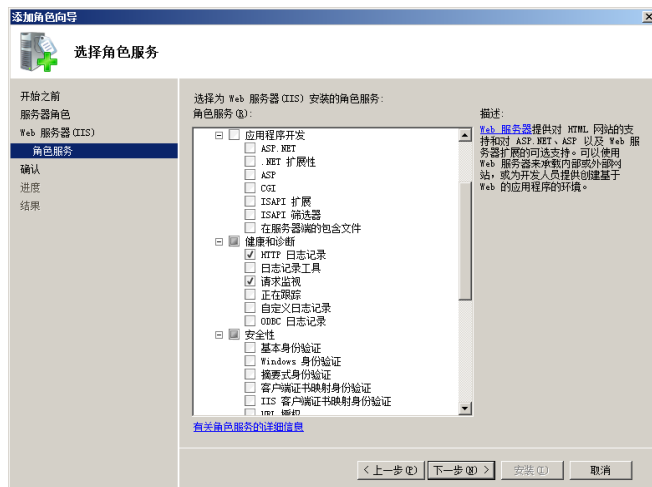


图 8-1 “选择角色服务”对话框



图 8-2 ApplicationHost.config 文件

3. 远程管理

IIS 管理员可以为其他用户授予远程管理权限，用户可以是具备 Windows 身份的用户，或者由 IIS 管理员临时指定的非 Windows 身份的用户。允许授予管理的目标包括 IIS 服务器、站点及应用程序，“IIS 管理器权限”窗口如图 8-3 所示。



图 8-3 “IIS 管理器权限”窗口

4. MMC 3.0 管理界面

IIS 管理器和以前的版本不同，将统一使用 MMC 3.0 版本的操作界面。在 IIS 管理器窗口中左侧为树型分级菜单；中部区域是功能面板；右侧区域为针对某个功能面板的操作任务区，其中显示所选服务或功能相关组件的常见任务，如图 8-4 所示。



图 8-4 IIS 7.0 管理界面

8.2 搭建与管理 Web 服务

在 Windows Server 2008 中可通过“添加角色向导”来安装 Web 服务器，并且所有的组件都可以在安装过程中定制。安装完成以后可以通过 IIS 7.0 管理，例如设置 IP 地址和端口、主目录及扩展服务等。

8.2.1 安装 Web 服务器

在 Windows Server 2008 服务器中安装 IIS 之前，应确认以下几个准备事项。

- (1) 为 IIS 服务器指定 IP 地址。
- (2) 为 Web 网站指定 DNS 域名，并注册到 DNS 服务器内。
- (3) Web 网页最好保存在 NTFS 分区内，以便设置 NTFS 权限来增加网页安全性。

如果要为 Internet 提供服务，所使用的域名必须是在 Internet 中申请的合法域名，这样用户才能通过 Internet 解析网站 IP 地址并访问。如果 Web 服务器只在 Intranet 中使用，则可自定义域名，并且应将局域网中客户端计算机的“首选 DNS 服务器”设置为 DNS 服务器的 IP 地址，这样才通过此 DNS 服务器解析网站的 IP 地址。

安装 Web 服务器的操作步骤如下。

- ① 在“服务器管理器”控制台中运行“添加角色向导”，在如图 8-5 所示的“选择服务器角色”对话框中选择待安装的角色。
- ② 选择“Web 服务器 (IIS)”复选框，显示如图 8-6 所示的“是否添加 Web 服务器 (IIS) 所需的功能”对话框。提示在安装 IIS 时，必须同时安装“Windows 进程激活服务”。

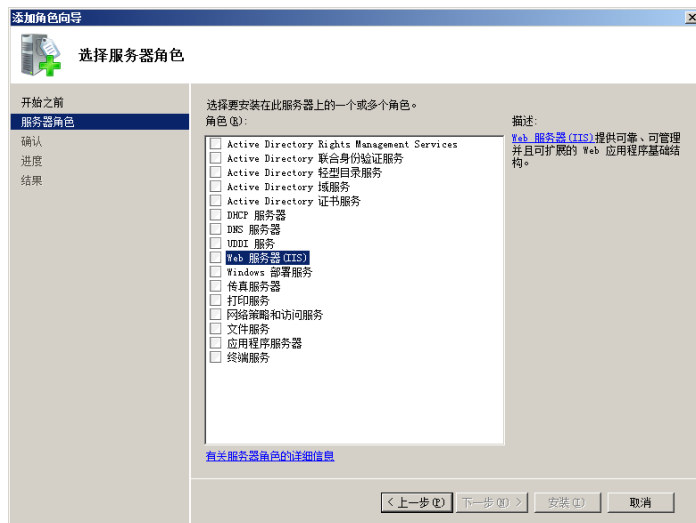


图 8-5 “选择服务器角色”对话框

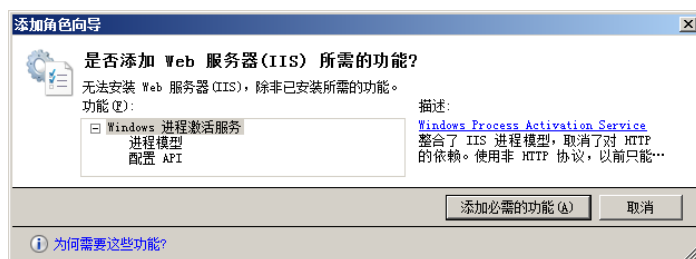


图 8-6 “是否添加 Web 服务器 (IIS) 所需的功能”对话框

③ 单击“添加必需的功能”按钮安装该功能，并选中“Web 服务器 (IIS)”复选框。单击“下一步”按钮，显示如图 8-7 所示的“Web 服务器 (IIS)”对话框，其中显示 Web 服务器的简介信息。



图 8-7 “Web 服务器 (IIS)”对话框

④ 单击“下一步”按钮，显示如图 8-8 所示的“选择角色服务”对话框。其中详细列出 Web 服务器所包含的组件模式，并且默认选中 Web 服务器的必需组件。

⑤ 如果要安装 ASP.NET 和 ASP 功能，则选中“ASP.NET”复选框。同时显示如图 8-9 所示的提示框，提示需要安装的组件。

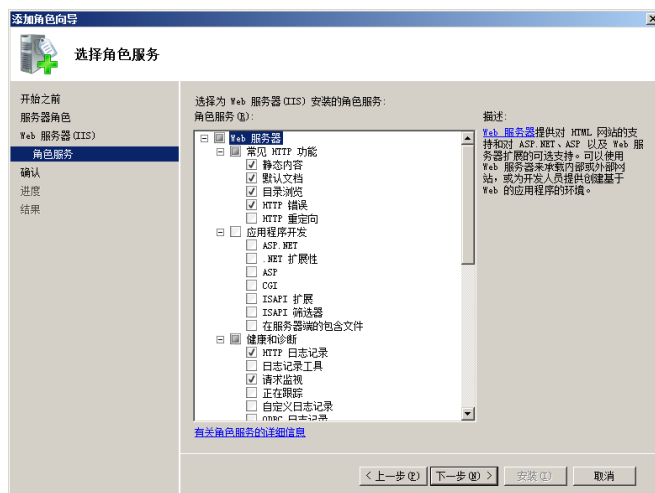


图 8-8 “选择角色服务”对话框

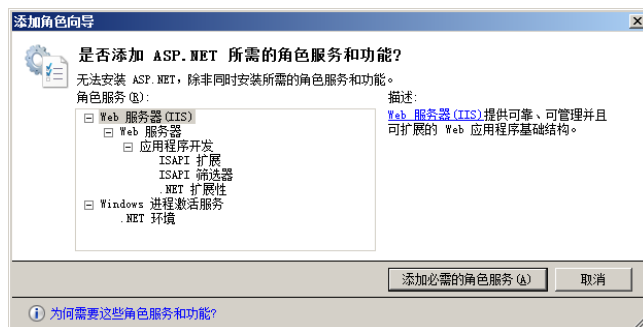


图 8-9 提示框

⑥ 单击“添加必需的角色服务”按钮，即可选中“ASP.NET”复选框。同时选中“ASP”复选框，如图 8-10 所示。

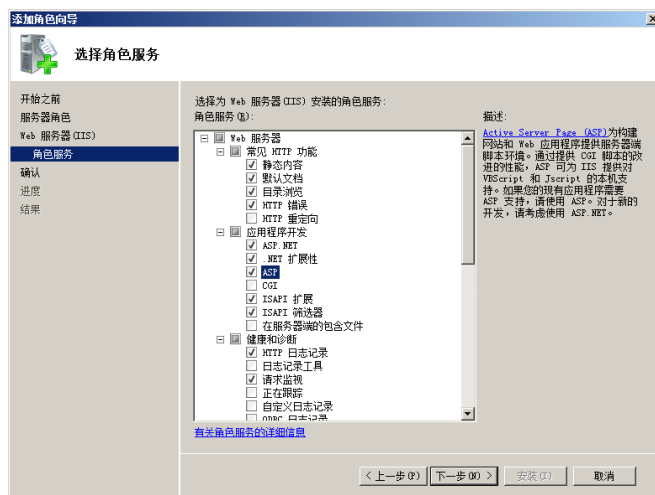


图 8-10 安装 ASPNET 和 ASP

⑦ 单击“下一步”按钮，显示如图 8-11 所示的“确认安装选择”对话框，其中列出所有准备安装的组件。

⑧ 单击“安装”按钮，开始安装 Web 服务器。安装完成后，显示如图 8-12 所示的“安装结果”对话框。



图 8-11 “确认安装选择”对话框



图 8-12 “安装结果”对话框

⑨ 单击“关闭”按钮，Web 服务器安装完成。单击“开始”→“管理工具”→“Internet 信息服务(IIS)管理器”选项，打开如图 8-13 所示的 IIS 管理器窗口，即可看到已安装的 Web 服务器及默认创建的 Web 站点。选择默认站点，在“Default Web Site 主页”窗口中即可配置站点的所需选项。

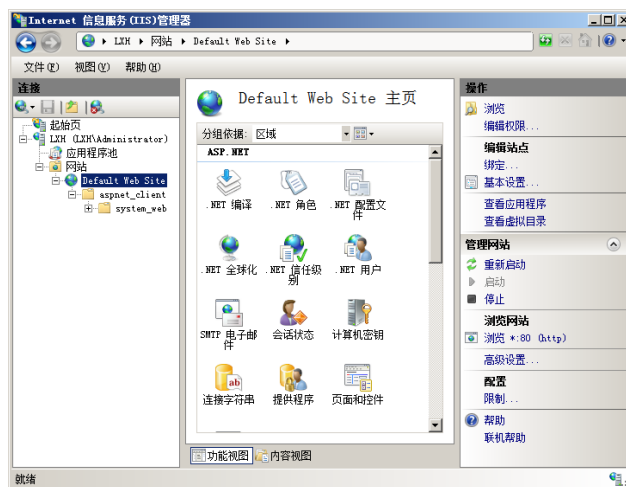


图 8-13 IIS 管理器窗口

此时，在客户端上打开 IE 浏览器，在地址栏中输入 Web 服务器的 IP 地址并按回车键。如果显示如图 8-14 所示的窗口，说明 Web 服务器安装成功；否则说明安装不成功，需要重新检查服务器及 IIS 设置。



图 8-14 Web 服务器安装成功

8.2.2 配置 IP 地址和端口

Web 服务器安装完成以后，可以使用默认创建的 Web 站点来发布 Web 网站。如果服务器中绑定有多个 IP 地址，则需要为 Web 站点指定唯一的 IP 地址及端口。

① 在 IIS 管理器中选择默认站点，右击并选择快捷菜单中的“编辑绑定”选项。或者单击右侧“操作”窗口中的“绑定”超级链接，显示如图 8-15 所示的“网站绑定”对话框。默认端口为 80，使用本地计算机中的所有 IP 地址。

② 选择该网站，单击“编辑”按钮显示如图 8-16 所示的“编辑网站绑定”对话框，在“IP 地址”下拉列表框中选择待指定的 IP 地址。在“端口”文本框中可以设置 Web 站点的端口号，并且不能为空。“主机名”文本框用来设置用户访问该 Web 网站时的名称，此时可保留为空。

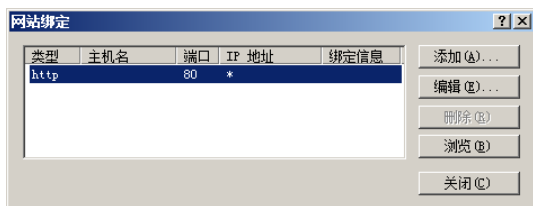


图 8-15 “网站绑定”对话框

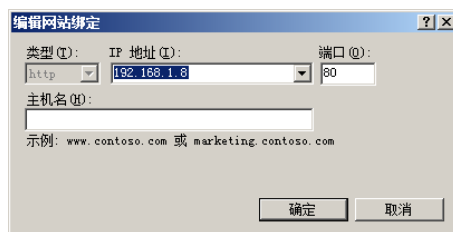


图 8-16 “编辑网站绑定”对话框



提示

使用默认的 80 端口时，用户访问该网站不需输入端口号，例如 `http://192.168.0.1` 或 `http://www.coolpen.net`；如果端口号不是 80，那么访问 Web 网站时必须提供端口号，例如 `http://192.168.0.1:8000` 或 `http://www.coolpen.net:8000`。

③ 设置完成以后，单击“确定”按钮保存设置，并单击“关闭”按钮关闭窗口。此时在 IE 浏览器的地址栏中输入 Web 服务器的地址，显示如图 8-17 所示的窗口，表示可以访问 Web 网站。

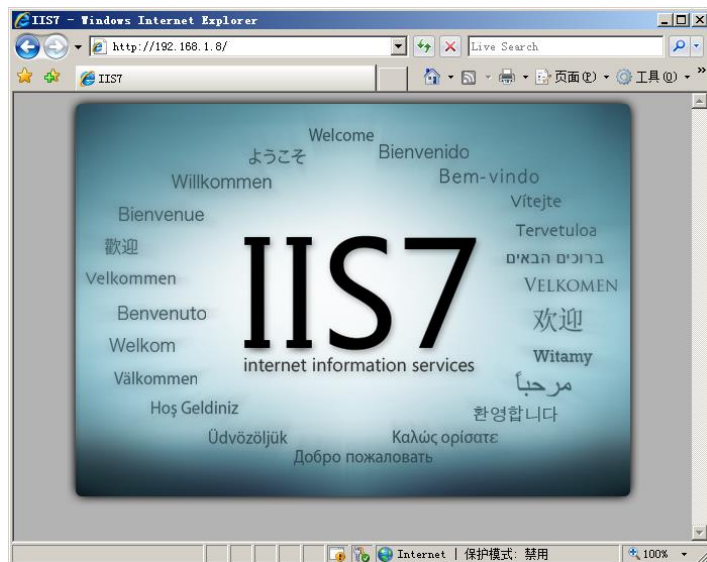


图 8-17 可以访问 Web 网站

8.2.3 配置主目录

主目录即网站的根目录，用来保存 Web 网站的网页及图片等数据，默认路径为“C:\inetpub\wwwroot”文件夹。不过，数据文件和操作系统放在同一磁盘分区中会失去安全保障，并可能影响系统运行，因此应设置为其他磁盘或分区。

① 打开 IIS 管理器，选择待设置主目录的站点。在右侧的“操作”窗格中单击“基本设置”超级链接，显示如图 8-18 所示的“编辑网站”对话框，在“物理路径”文本框中显示网站的主目录。

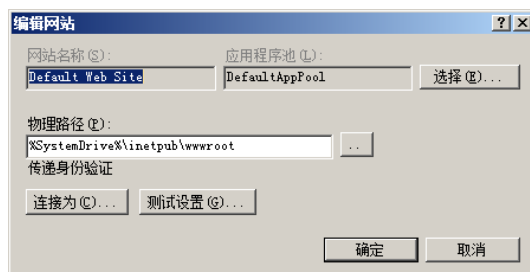


图 8-18 “编辑网站”对话框

② 在“物理路径”文本框中键入 Web 站点的新主目录路径或者单击“浏览”按钮选择，最后单击“确定”按钮保存设置。

8.2.4 配置默认文档

用户访问网站时通常只需输入网站域名即可，无须输入网页名，而实际上此时显示的网页就是默认文档。一般情况下，Web 网站需要至少一个默认文档，当用户使用 IP 地址或域名访问且没有输入网页名时，Web 服务器就会显示默认文档的内容。

① 在 IIS 管理器中选择默认站点，在窗口中间的默认站点主页中双击“IIS”选项区域的“默认文档”图标，显示如图 8-19 所示的“默认文档”窗口。有 5 种默认文档，分别为 Default.htm、Default.asp、index.htm、index.html 和 iisstar.htm。当用户访问时，IIS 会自动按顺序由上至下依次查找与之相对应的文档名。

② 单击右侧“操作”任务栏中的“添加”超级链接，显示如图 8-20 所示的“添加默认文档”对

话框，在“名称”文本框中键入待添加的默认文档名。

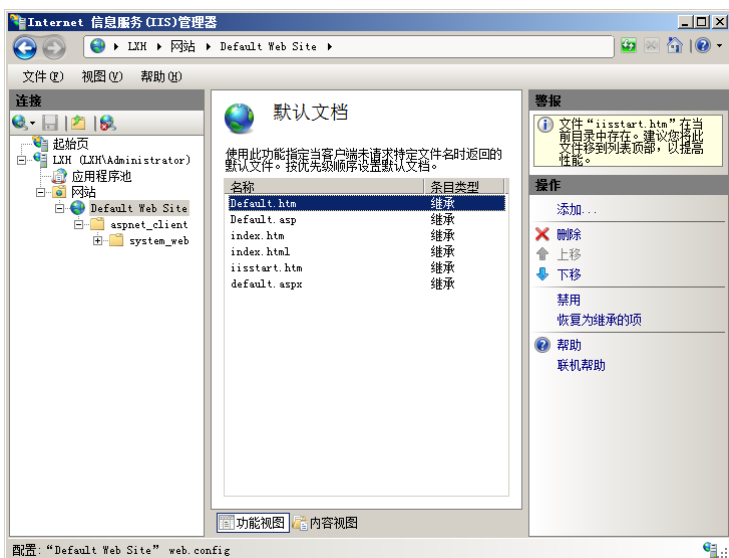


图 8-19 “默认文档”窗口



图 8-20 “添加默认文档”对话框

③ 单击“确定”按钮，添加该默认文档。新添加的默认文档自动排列在最上方，如图 8-21 所示，可通过“上移”和“下移”超级链接来调整各个默认文档的顺序。

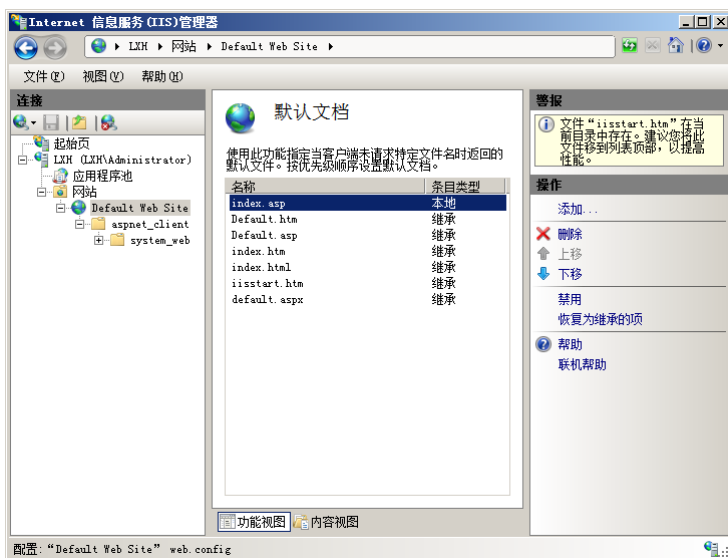


图 8-21 新添加的默认文档

如果需要删除或禁用某个默认文档，只需选择相应的默认文档，然后单击“删除”或“禁用”超级链接。

8.2.5 配置访问权限和安全

默认状态下允许所有的用户匿名连接 IIS 网站，即访问时不需要使用用户名和密码登录。如果对网站的安全性要求高，或网站中有机密信息，则需要禁止匿名用户访问，而只允许特殊的用户账户访问。

1. 禁止匿名访问

① 在 IIS 管理器中选择待设置身份验证的 Web 站点，如图 8-22 所示。

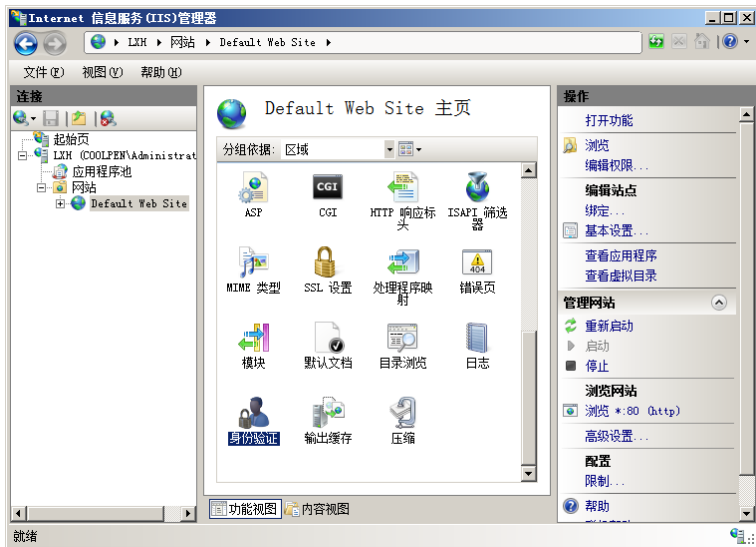


图 8-22 选择待设置身份验证的 Web 站点

② 在站点主页窗口中双击“身份验证”图标，显示如图 8-23 所示的“身份验证”窗口。默认情况下，“匿名身份验证”为“启用”状态。

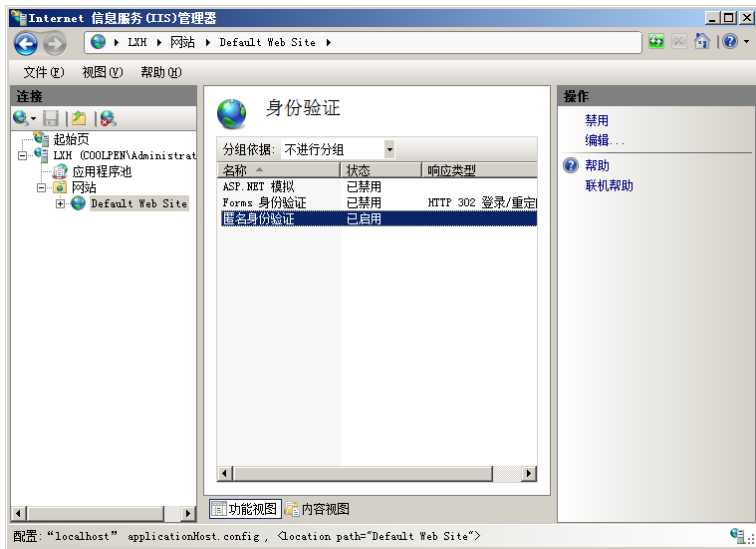


图 8-23 “身份验证”窗口

③ 右击“匿名身份验证”选项，选择快捷菜单中的“禁用”选项，即可禁止匿名用户访问。

2. 使用身份验证

在 IIS 7.0 的身份验证方式中，提供基本验证、Windows 身份验证和摘要身份验证。需要注意的是，一般在禁止匿名访问时才使用其他验证方法。不过在默认安装方式下，这些身份验证方法并没有安装，可在安装过程中或者安装完成后手动安装。

① 在“服务器管理器”窗口中展开“角色”选项，选择“Web 服务器 (IIS)”选项。单击“添加角色服务”选项，显示如图 8-24 所示的“选择角色服务”对话框，在“安全性”选项区域中选择待安装的身份验证方式。

② 安装完成后打开 IIS 管理器，打开如图 8-25 所示的“身份验证”窗口。所安装的身份验证方式显示在列表中，并且默认均为禁用状态。

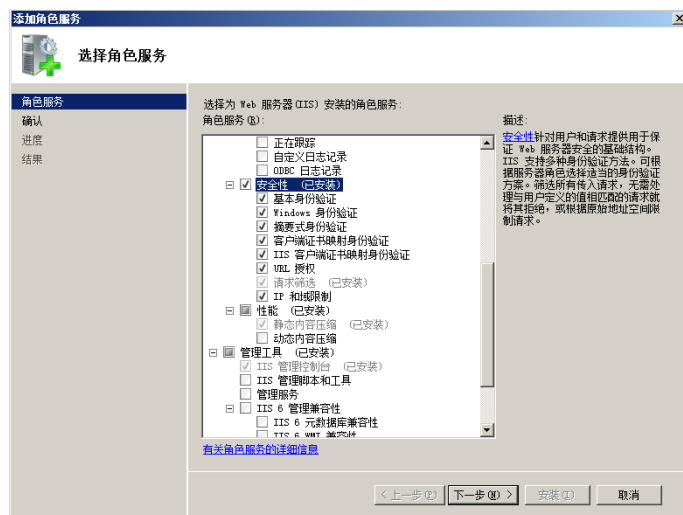


图 8-24 “选择角色服务”对话框



图 8-25 “身份验证”窗口

可安装的身份验证方式共有如下 3 种。

- 基本身份验证：该验证会“模仿”为一个本地用户（即实际登录到服务器的用户）在访问 Web 服务器时登录。因此如果以基本验证方式确认用户身份，用于基本验证的 Windows 用户必须具有“本地登录”用户权限。默认情况下，Windows 主域控制器（PDC）中的用户账户不授予“本地登录”用户的权限。但使用基本身份验证方法将导致密码以未加密形式在网络上传输，蓄意破坏系统安全的黑客可以在身份验证过程中使用协议分析程序破译用户和密码。
- 摘要式身份验证：该验证只能在带有 Windows 域控制器的域中使用，域控制器必须具有所用密码的纯文本复件，因为必须执行散列操作并将结果与浏览器发送的散列值相比较。
- Windows 身份验证：集成 Windows 身份验证是一种安全的验证形式，它需要用户输入用户名和密码。但用户名和密码在通过网络发送前会经过散列处理，因此可以确保安全性。当启用这种验证时，用户的浏览器通过 Web 服务器进行密码交换。Windows 身份验证使用 Kerberos v5 验证和 NTLM 验证，如果在 Windows 域控制器上安装了 Active directory 服务并且用户的浏览器支持 Kerberos v5 验证协议，则使用 Kerberos v5 验证；否则使用 NTLM 验证。

Windows 身份验证优先于基本验证，但并不提示用户输入用户名和密码。只有验证失败后，浏览器才提示用户输入用户名和密码。Windows 身份验证非常安全，但是在通过 HTTP 代理连接时不起作用，无法在代理服务器或其他防火墙应用程序后使用，因此这种身份验证最适合企业 Intranet 环境。

例如，当 Web 服务器使用基本身份验证并在客户端访问该网站时，会提示如图 8-26 所示的“连接到 www.coolpen.net”对话框。在用户名和密码文本框中输入合法的用户名及密码，单击“确定”按钮即可打开网页。



图 8-26 “连接到 www.coolpen.net”对话框

3. 通过 IP 地址限制保护网站

在 IIS 中可以通过限制 IP 的方式来增加网站的安全性，即通过允许或拒绝来自特定 IP 地址的访问有效地避免非法用户的访问。不过，这种方式只适合于向特定用户提供 Web 网站的情况。同样，“IP 地址限制”功能也需要手动安装，为此在“选择角色服务”对话框中选“IP 和域限制”复选框。

① 设置允许访问的 IP 地址

- 打开 IIS 管理器，选择待限制的 Web 站点。双击“IPv4 地址和域限制”图标，显示如图 8-27 所示的“IPv4 地址和域限制”窗口。

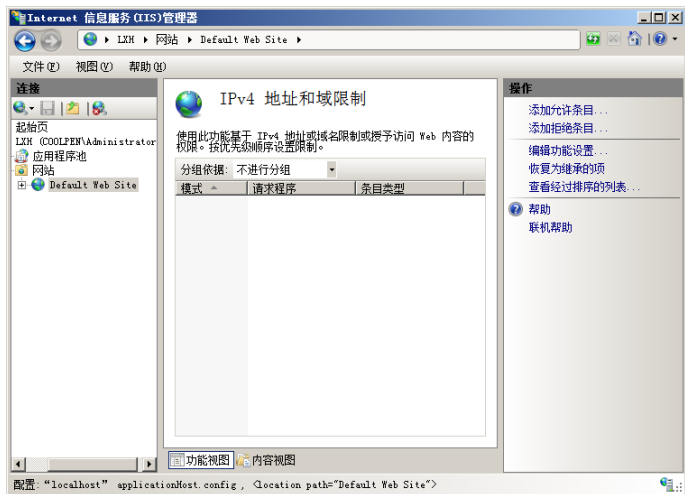


图 8-27 “IPv4 地址和域限制”窗口

- 在右侧“操作”窗格中单击“添加允许条目”按钮，显示如图 8-28 所示的“添加允许限制规则”对话框。如果要添加一个 IP 地址，则选择“特定 IPv4 地址”单选按钮，并键入允许访问的 IP 地址；如果要添加一个 IP 地址段，则选择“IPv4 地址范围”单选按钮，并键入 IP 地址及子网掩码。
- 单击“确定”按钮，IP 地址添加完成。

② 设置拒绝访问的计算机

“拒绝访问”与“允许访问”正好相反，通过“拒绝访问”设置将拒绝来自一个 IP 地址或 IP 地址段的计算机访问 Web 站点。不过，已授予访问权限的计算机仍可访问。单击“添加拒绝条目”按钮，

打开如图 8-29 所示的“添加拒绝限制规则”对话框。在其中添加拒绝访问的 IP 地址，操作步骤与添加允许条目相同，这里不再赘述。

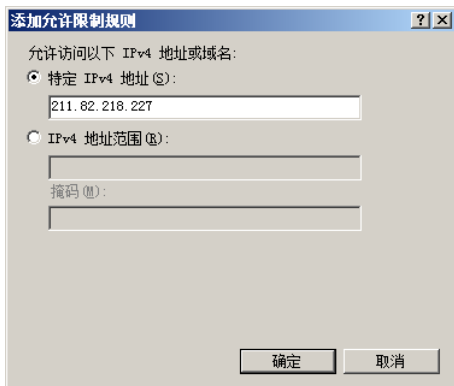


图 8-28 “添加允许限制规则”对话框

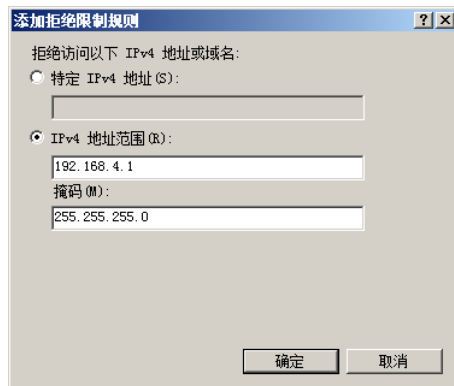


图 8-29 “添加拒绝限制规则”对话框

8.2.6 配置自定义错误

有时可能会因为网络或者 Web 服务器设置的原因，而使得用户无法正常访问 Web 页。为了能够使用户清楚地了解不能访问的原因，在 Web 服务器上应设置相应的反馈给用户的错误页。错误页可以是自定义的，也可以包含排除故障原因的详细错误信息。

默认情况下，IIS 已经集成了一些常见的错误代码。在“Default Web Site 主页”窗口中单击“错误页”图标，显示如图 8-30 所示的“错误页”窗口，其中显示一些常用的错误代码信息。

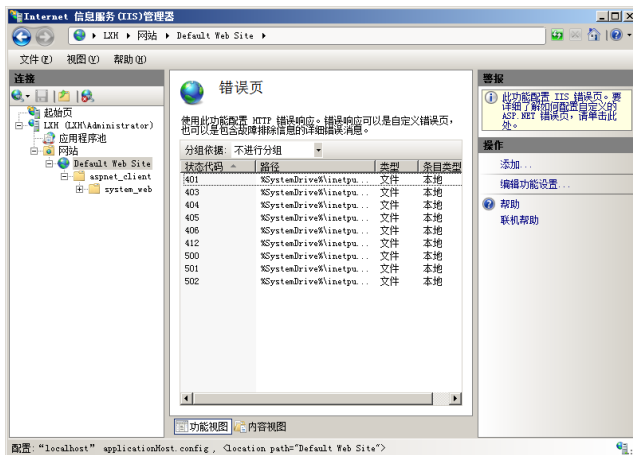


图 8-30 “错误页”窗口

如果需要更改某个错误页代码号，则右击代码名称。选择快捷菜单中的“更改状态”选项，则错误页代码号变为可改写状态，重新键入新的代码号即可。

如果要查看或修改错误页代码信息，则选择一个错误页代码。右击并选择快捷菜单中的“编辑”选项，或者单击“编辑”超级链接，显示如图 8-31 所示的“编辑自定义错误页”对话框。在其中可定义发生该错误时返回给用户的信息，或者发生该错误时所执行的操作。

其中的选项如下。

(1) 将静态文件中的内容插入错误响应中：在“文件路径”文本框中可设置当发生错误时返回给客户端的 Web 页。如果选中“尝试返回使用客户端语言的错误文件”复选框，可以根据客户端所使用的不同语言页返回相应的错误页。

(2) 在此网站上执行 URL：选择该单选按钮，可在“URL（相对于网站根目录）”文本框中键入相对于网站根目录的相对路径中的错误页，如“/ErrorPages/404.aspx”。

(3) 以 302 重定向响应：选择该单选按钮，可在“绝对 URL”文本框中键入当发生该错误时重定向的网站地址。

虽然 IIS 自带了一些错误页代码，但并不一定能满足用户的所有需要，因此可以自定义添加一些错误页代码。在“错误页”窗口中单击“添加”按钮，显示如图 8-32 所示的“添加自定义错误页”对话框。在“状态代码”文本框中设置一个错误页代码号，根据需要在“响应操作”选项组中设置当发生错误时的响应操作。最后，单击“确定”按钮保存设置。

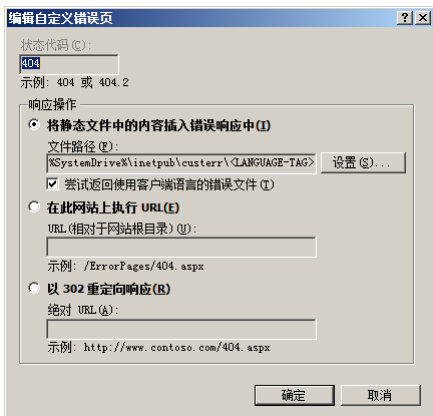


图 8-31 “编辑自定义错误页”对话框

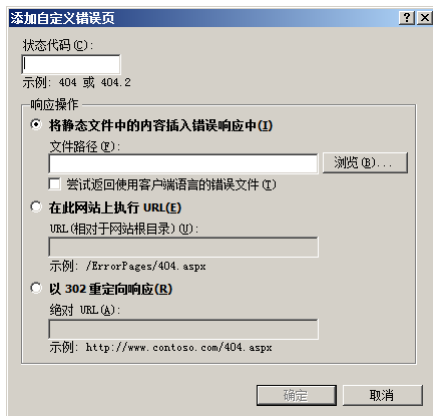


图 8-32 “添加自定义错误页”对话框

8.2.7 配置 MIME 类型

MIME (Multipurpose Internet Mail Extensions, 多功能 Internet 邮件扩充服务) 是一种保证非 ASCII 码文件在 Internet 上传播的标准，最早用于邮件系统传送图片等非 ASCII 的内容，如今浏览器也支持这种规范。如果 Web 服务器中没有添加相应的 MIME 类型，则用户无法访问该类型的文件。

① 在 IIS 管理器中，选择 Web 站点主页。双击“MIME 类型”图标，显示如图 8-33 所示的“MIME 类型”窗口，其中列出系统已经集成的 MIME 类型。



图 8-33 “MIME 类型”窗口

② 如果需要添加新的 MIME 类型，则在“操作”窗格中单击“添加”按钮，显示如图 8-34 所示的“添加 MIME 类型”对话框。在“文件名扩展名”文本框中键入要添加的 MIME 类型，例如“.iso”，在“MIME 类型”文本框中键入文件扩展名所属的类型。

③ 单击“确定”按钮，MIME 类型添加完成。如果还要添加其他 MIME 类型，可按如上步骤继续操作。



图 8-34 “添加 MIME 类型”对话框

8.2.8 配置安全 Web 服务

为了保护 Web 网站的安全，防止数据在传输过程中被截获和篡改，可以在 Web 服务器上配置 SSL (Secure Socket Layer，安全套接字层)。SSL 是一种利用证书实现数据加密的技术，HTTP 协议可用来加密传输对安全比较敏感的数据和信息，实现 Web 服务端与 Web 客户端的安全通信。而客户端访问时，则使用“https://DNS 域名或 IP 地址”的形式。

1. 创建 SSL 证书

由于 SSL 是利用证书实现数据加密传输，因此要使用 SSL，必须在 Web 服务器端创建用于 SSL 加密的证书，其中包含有关服务器的信息。服务器允许客户在共享敏感信息之前对其加以识别，Web 服务器只有安装有效服务器证书后才拥有安全通信功能。

① 在“Internet 信息服务 (IIS) 管理器”窗口中选择服务器名称，在“主页”中的“IIS”区域中双击“服务器证书”图标，显示如图 8-35 所示的“服务器证书”窗口。在安装 IIS 7.0 时，系统自动创建了一个证书。网络管理员可以直接应用该证书实现 SSL，也可以导入已有证书或者创建新证书。

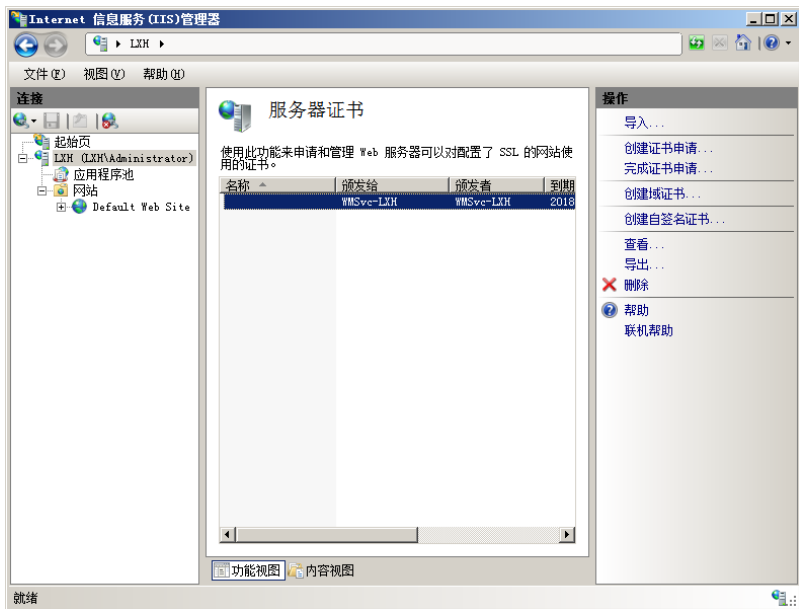


图 8-35 “服务器证书”窗口

② 这里以创建一个自签名证书为例，在“操作”窗格中单击“创建自签名证书”超级链接，显示如图 8-36 所示的“创建证书申请”对话框，在“为证书指定一个好记的名称”文本框中为新证书键入一个名称。

③ 单击“确定”按钮，自签名证书创建完成并显示在证书列表中，如图 8-37 所示。

④ 选择新创建的证书并单击“查看”超级链接，显示如图 8-38 所示的“证书”对话框。在其中可以查看该证书的名称、颁发者、颁发给、到期日期和证书哈希等详细信息，单击“确定”按钮。

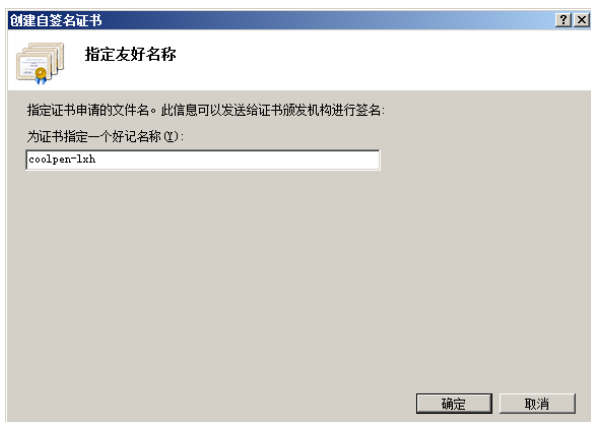


图 8-36 “创建自签名证书”对话框

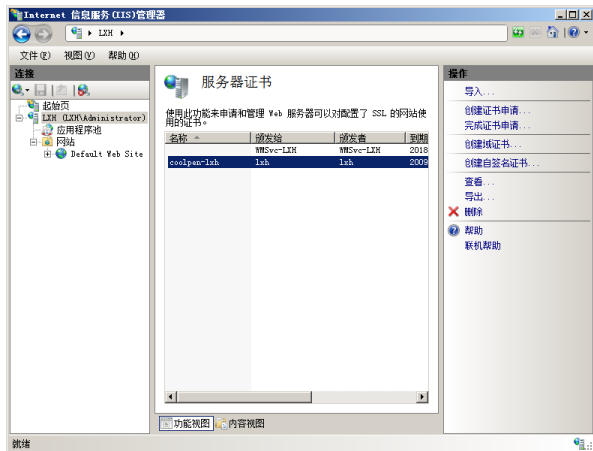


图 8-37 创建完成的证书

2. 创建 SSL 网站

当创建完成 SSL 证书后即可创建 HTTPS 站点，并启用 SSL 设置。需要注意的是，HTTPS 站点只能在创建 SSL 证书后创建，不能将已创建的 HTTP 站点更改为 HTTPS 站点。

① 在 IIS 管理器窗口的“连接”栏中右击“网站”并选择快捷菜单中的“添加网站”选项，显示如图 8-39 所示的“添加网站”对话框。在“类型”下拉列表框中选择“https”选项，在“IP 地址”下拉列表框中指定 IP 地址，“端口”使用默认的 443 即可，在“SSL 证书”下拉列表框中选择该网站使用的证书。

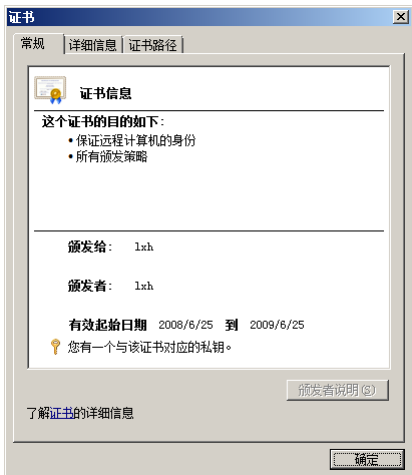


图 8-38 “证书”对话框

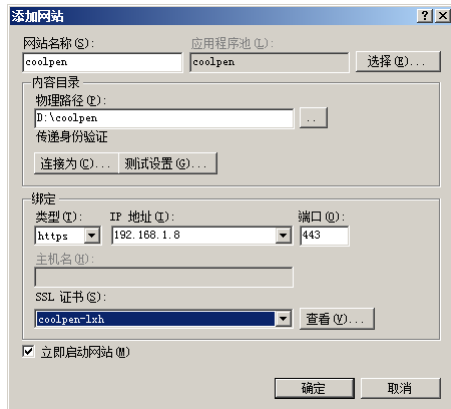


图 8-39 “添加网站”对话框

② 单击“确定”按钮，创建完成 HTTPS 网站，如图 8-40 所示。

③ 在 HTTPS 网站主页中双击“IIS”区域中的“SSL 设置”图标，显示如图 8-41 所示的“SSL 设置”窗口。

④ 选中“要求 SSL”复选框，默认启用 40 位数据加密方法。如果选中“需要 128 位 SSL”复选框，则启动 128 位数据加密方法。在“客户证书”选项区域中选择 3 种证书接受方式。

- 忽略：系统默认设置，不接受提供客户端证书，因此安全性也最低。
- 接受：启用服务器端的 SSL 设置并接受客户端证书（若提供），在允许客户端获得内容访问权限之前验证客户端身份，这里选择该单选按钮。
- 必需：在接受用户访问之前要求提供证书，以验证客户端身份的有效性，安全性最高。

设置完成后，在“操作”窗格中单击“应用”超级链接，应用所做的设置，如图 8-42 所示。



图 8-40 创建完成 HTTPS 网站

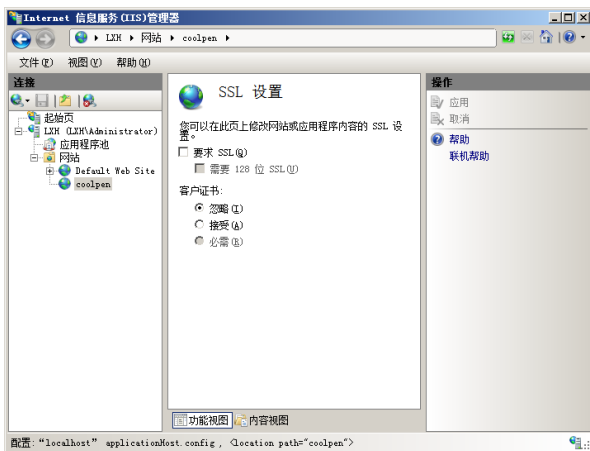


图 8-41 “SSL 设置”窗口

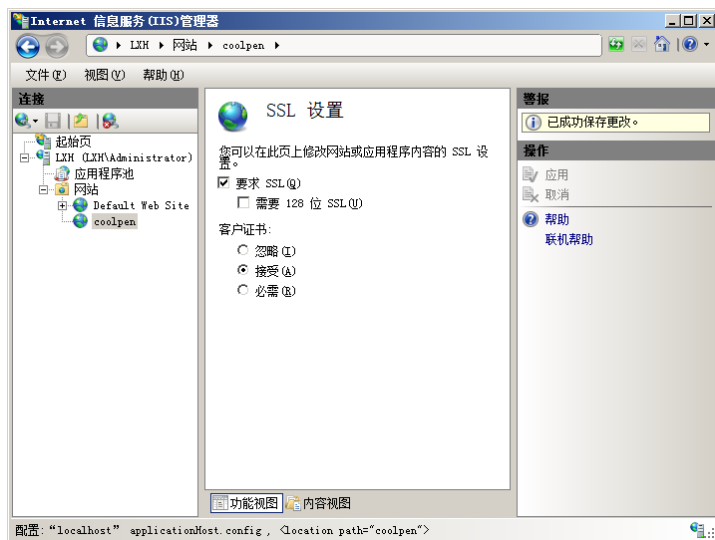


图 8-42 应用 SSL 设置

8.2.9 启动与停止 Web 服务器

如果需要暂时停止某个网站的运行，可在 IIS 管理器中选择要停止的网站。右击并选择快捷菜单中的“管理网站”→“停止”选项即可将该网站停止，用户将不能访问该网站。

如果需要启动已停止的网站，可右击该网站并选择快捷菜单中的“管理网站”→“启动”选项，即可再次启动该网站，用户仍可继续访问。如果选择快捷菜单中的“管理网站”→“重新启动”选项，则可重新启动网站。尤其在维护网站时比较有用，例如添加新的应用程序等。

8.3 创建与管理虚拟网站

由于企业中的部门及用户比较多，有些部门需要建立各自的独立网站，有些用户也想建立个人网站，提供个人主页服务。但限于成本，不可能，也没有必要为每个网站都使用一台服务器。此时可以利用虚拟网站来实现，即在一台服务器上搭建多个网站，并且可以分别拥有各自的 IP 地址或域名。而在用户看来，就好像这些网站分别位于不同的服务器。

8.3.1 虚拟网站概述

利用虚拟 Web 网站功能可以在一台服务器上创建和管理多个 Web 站点，从而节省设备投资且便

于集中管理，这是中小型企业理想的网站搭建方式。虚拟网站主要具有以下特点。

(1) 节约投资：由于多个虚拟 Web 站点可以运行在同一台服务器上，因此为企业节省了软件和硬件投资。不过，在虚拟 Web 网站中需要为每个域名分配一个唯一的 IP 地址，其性能和表现都与独立的 Web 服务器类似。

(2) 便于管理：虚拟 Web 服务器与真正的 Web 服务器相比，配置和管理方式基本相同，而且可以使用 Web 方式远程管理。

(3) 数据安全：对于敏感数据，可以利用虚拟 Web 服务器将其隔离，从而提高了数据安全性。

(4) 分级管理：不同的虚拟网站可以指定不同的管理人员，同一虚拟网站也可以指定若干管理人员。将 Web 站点层层委派给享有相应权限的人员管理使每一个部门都有自己的虚拟服务器，并且能够完全管理自己的站点。

(5) 性能和带宽调节：当计算机中安装有若干个虚拟网站时可以为每一个虚拟 Web 站点分配性能和带宽，以保证服务器的稳定运行，合理分配网络带宽和 CPU 处理能力。

(6) 创建虚拟目录：在虚拟 Web 站点上同样可以创建虚拟目录，使虚拟 Web 的磁盘容量和信息内容趋于无穷大。

8.3.2 虚拟网站创建方式

在一台服务器上创建多个虚拟站点最常用方式有 3 种，分别是主机头名法、端口法和 IP 地址法，3 种方法的区别如下。

(1) 使用 IP 地址创建：只要服务器绑定有多个 IP 地址，就可以利用为每个虚拟网站分配一个独立的 IP 地址，用户可通过访问 IP 地址来访问相应的网站。

(2) 使用端口号创建：如果服务器只有一个 IP 地址，就可以使用同一个 IP 地址及不同的 TCP 端口来创建虚拟网站。不过，用户必须加上相应的端口号才能访问。

(3) 使用主机头名创建：这是最常用的创建虚拟 Web 网站的方法，也最便于用户的访问。如果服务器上只有一个 IP 地址，即可添加多个不同主机头名的网站，用户访问时仍使用 DNS 域名访问。

Windows Server 2003 中的 IIS 6.0 和 Windows Server 2008 中的 IIS 7.0 均支持虚拟网站功能，在 IIS 管理器中选择“网站”选项，显示“网站”窗口。在其中可创建虚拟网站，所有创建的新虚拟网站也都会显示在该窗口中，如图 8-43 所示。

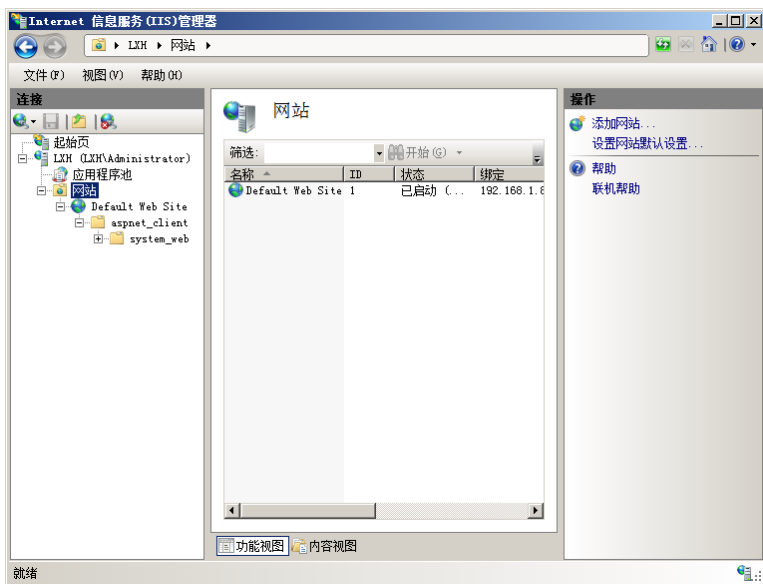


图 8-43 创建的新虚拟网站

8.3.3 使用 IP 地址创建

如果服务器网卡绑定有多个 IP 地址，则可以为新虚拟网站分配一个 IP 地址，使用户利用 IP 地址即可访问该网站。

① 在 IIS 管理器的“网站”窗口中右击“网站”选项并选择快捷菜单中的“添加网站”选项，显示如图 8-44 所示的“添加网站”对话框。

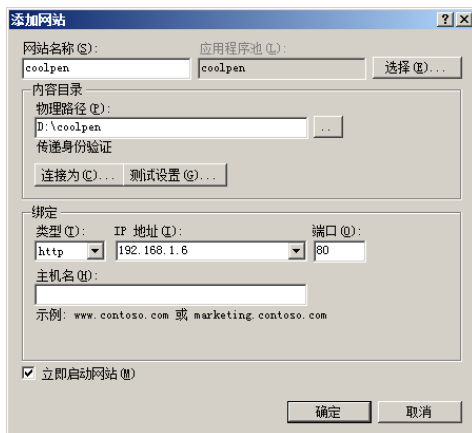


图 8-44 “添加网站”对话框

在其中设置如下选项。

- 网站名称：为虚拟网站设置一个名称，以便与其他网站相区分。
- 物理路径：为虚拟网站指定主目录路径。
- IP 地址：为虚拟网站指定一个 IP 地址。

② 设置完成后单击“确定”按钮，创建完成一个新的虚拟网站，如图 8-45 所示，用户使用所分配的 IP 地址即可访问 Web 网站。

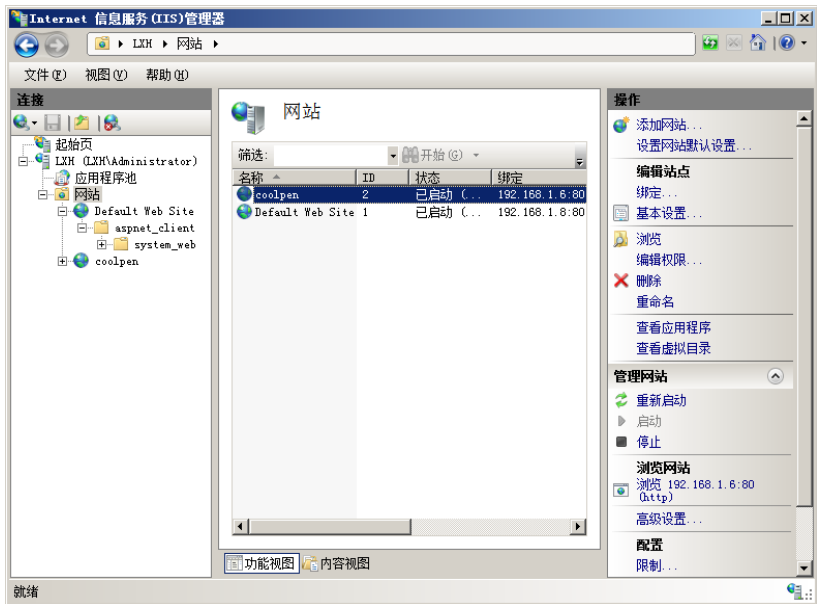


图 8-45 使用 IP 地址创建的虚拟网站

8.3.4 使用端口号创建

通过为虚拟网站分配不同的端口号，也可以实现一台服务器搭建多个虚拟网站的目的。不过，用

户访问该网站时必须加上端口号，格式为“http://Web 网站域名和 IP 地址:端口号”，例如，http://192.168.1.7:85。而 Web 网站的默认端口号为 80，访问时不需使用端口号。

① 在 IIS 管理器的“网站”窗口中右击“网站”选项并选择快捷菜单中的“添加网站”选项，显示如图 8-46 所示的“添加网站”对话框，设置“网站名称”和“物理路径”。如果服务器只有一个 IP 地址，则保留“IP 地址”文本框中的默认“全部未分配”选项，并且指定 Web 网站所使用的 IP 地址。然后在“端口”文本框中键入新的端口号，如图 8-46 所示。

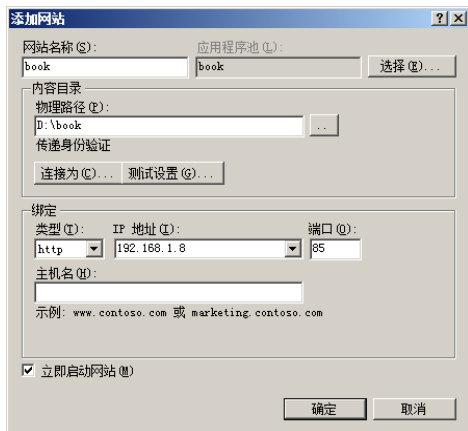


图 8-46 使用端口号创建虚拟网站

② 单击“确定”按钮，一个新虚拟网站创建完成。如果要创建多个虚拟网站，只需设置不同的端口即可。

8.3.5 使用主机头名创建

利用“主机头名”创建 Web 站点是目前使用最多的方法，只要有一个 IP 地址即可在一台服务器上发布多个不同域名的网站，从而可以合理地利用服务器资源。使用这种方式创建网站时应事先创建相应的 DNS 名称，用户在访问时只需使用相应的域名。

① 在 DNS 控制台台中将 IP 地址和域名注册到 DNS 服务器中，如图 8-47 所示。

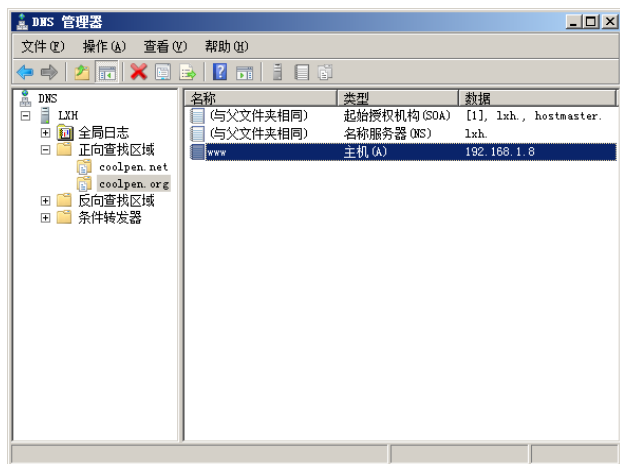


图 8-47 将 IP 地址和域名注册到 DNS 服务器中

② 在 IIS 管理器的“网站”窗口中，右击“网站”选项并选择快捷菜单中的“添加网站”选项，显示“添加网站”对话框。设置“网站名称”、“物理路径”及“IP 地址”，并在“主机名”文本框中键入已设置的主机头名，如图 8-48 所示。

③ 单击“确定”按钮，网站创建成功。可以在同一台服务器中创建多个不同主机头名的网站。

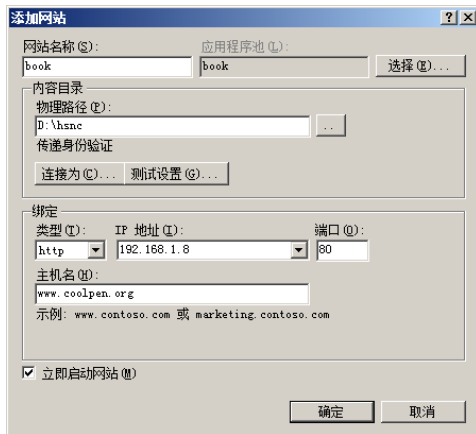


图 8-48 利用主机头名创建虚拟网站

8.3.6 管理虚拟网站

虚拟网站的管理方式和默认网站完成一样，在其相应的主页窗口中即可管理，如图 8-49 所示。



图 8-49 管理虚拟网站

8.4 创建与管理虚拟目录

虚拟目录也就是网站的子目录，和 Web 网站一样，其中保存了各种网页及数据，使用户可以像访问网站一样访问。利用虚拟目录，也可以像虚拟网站一样实现一台服务器发布多个网站的目的。

8.4.1 虚拟目录概述

虚拟目录实际上就是一个文件夹，并不一定位于 Web 网站的主目录内，甚至可能位于其他服务器中。但在用户看来，如同位于同一台服务器。虚拟目录是主网站的下一级目录，并且要依附于主网站，例如 <http://www.coolpen.net/book>。

虚拟目录具有以下意义。

(1) 便于扩展：由于网站可能需要升级，这时可以创建虚拟目录来增加新的网页内容；另外由于

Web 内容越来越多，需要扩展磁盘空间。这时就可以安装新磁盘并创建虚拟目录，而用户访问时就如同在同一个文件夹中。

(2) 增删灵活：可以根据需要随时在虚拟 Web 网站中添加虚拟目录，或者从网站中移除，灵活性很强。而且在添加或移除虚拟目录时，不会影响 Web 网站的运行。

(3) 易于配置：虚拟目录与主网站使用相同的 IP 地址、端口号和主机头名，因此不会产生冲突。同时新建的虚拟目录将自动继承宿主网站的配置，并且宿主网站的配置也将直接传递至虚拟目录，因此管理更加简单。

利用虚拟目录和虚拟网站都可以创建 Web 网站，但是虚拟网站是一个独立的网站，可以拥有独立的 DNS 域名、IP 地址或端口号；虚拟目录则需要挂接在某个虚拟网站下，并且没有独立的 DNS 域名、IP 地址或端口号，用户访问时必须带上相应的主网站名。

8.4.2 虚拟目录创建方式

虚拟目录可以在任何一个虚拟网站中创建，而且每个虚拟网站中可创建多个虚拟目录。

① 在 IIS 管理器中选择待创建虚拟目录的站点，右击并选择快捷菜单中的“添加虚拟目录”选项，显示如图 8-50 所示的“添加虚拟目录”对话框。在“别名”文本框中键入虚拟目录的别名，在“物理路径”文本框中键入该虚拟目录所在的物理路径。



图 8-50 “添加虚拟目录”对话框



虚拟目录的物理路径既可以是本地计算机的物理路径，也可以是网络中其他计算机中的共享文件夹。



② 单击“确定”按钮，虚拟目录添加成功，并显示在 Web 站点下方作为子目录。按照同样操作步骤，可以继续添加其他虚拟目录，另外在已创建的虚拟目录中也可以添加子虚拟目录。

在 Web 网站主页窗口中单击“操作”窗格中的“查看虚拟目录”超级链接，可查看所有已创建的虚拟目录，如图 8-51 所示。另外，单击“添加虚拟目录”超级链接也可创建虚拟目录。

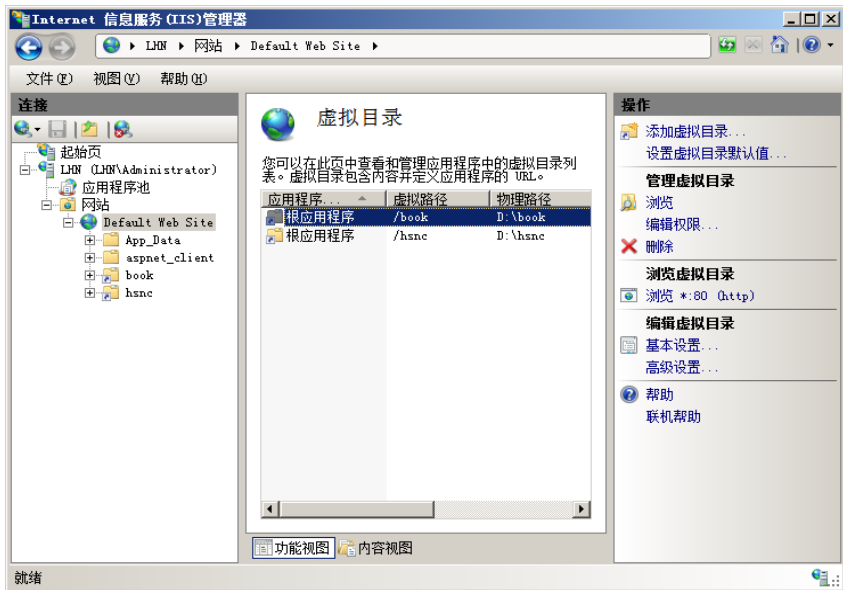


图 8-51 所有已创建的虚拟目录

8.4.3 管理虚拟目录

虚拟目录和主网站一样可以在主页中完成各种配置管理（如图 8-52 所示），并配置主目录、默认文档、MIME 类型，以及身份验证等，操作方法和主网站完全一样。所不同的是，不能为虚拟目录指定 IP 地址、端口号，以及 ISAPI 筛选器。

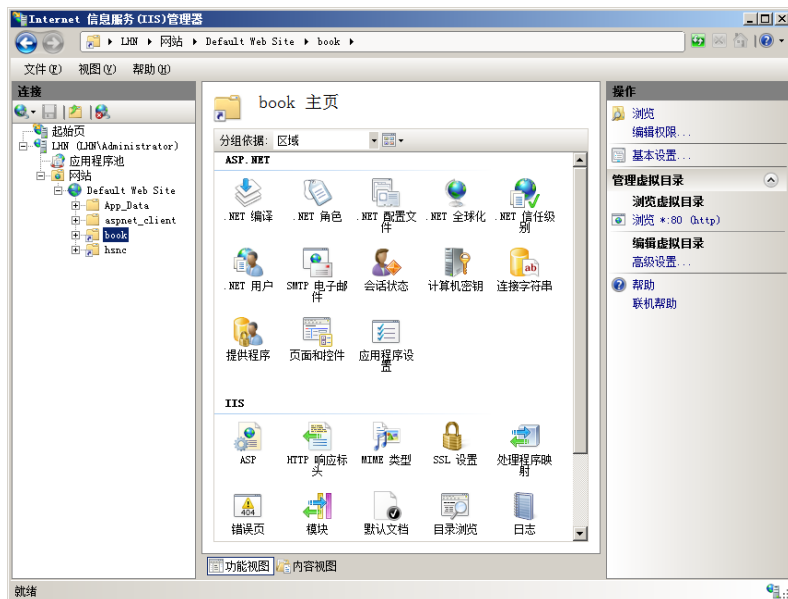


图 8-52 虚拟目录主页

8.5 安装与设置 Apache

Apache 是目前最流行的 Web 服务器软件，世界上半以上的 Web 服务器都是用其搭建的。它不仅具有相当高的可移植性，可运行于 Unix 及 Windows 等操作系统，而且性能高且资源占有率低。同时 Apache 还是一个自由的免费软件，可由用户自行修改开发。

8.5.1 安装 Apache

安装 Apache 的操作步骤如下。

- ① 运行下载的 Apache 安装程序，显示如图 8-53 所示的安装向导。
- ② 单击“Next”按钮，显示如图 8-54 所示的“License Agreement”对话框。选择“I accept the terms in the license agreement”单选按钮，接受许可协议。



图 8-53 Apache 安装向导

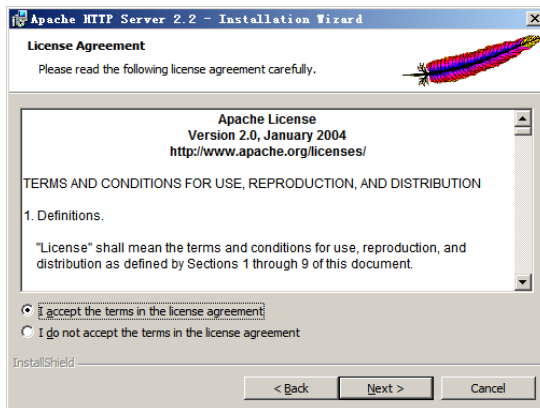


图 8-54 “License Agreement”对话框

③ 单击“I Agree”按钮，显示如图 8-55 所示的“Choose Components”对话框。在其中用户可以自定义所要安装的组件，也可以在“Select the type of install”下拉列表框中选择安装模式，默认为正常安装。

④ 单击“Next”按钮，显示如图 8-56 所示的“Read This First”对话框，在其中可以查看 Apache 的版本及使用说明。

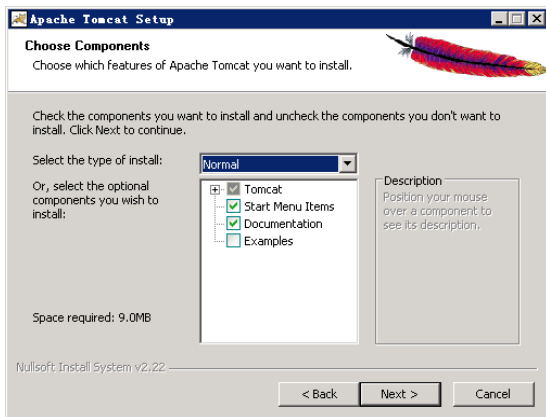


图 8-55 “Choose Components”对话框

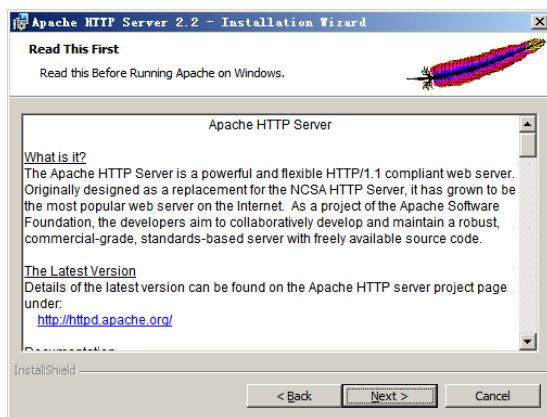


图 8-56 “Read This First”对话框

⑤ 单击“Next”按钮，显示如图 8-57 所示的“Server Information”对话框。在“Network Domain”文本框中输入域名，在“Server Name”文本框中输入服务器名，在“Administrator’s Email Address”文本框中输入管理员邮件地址。

⑥ 单击“Next”按钮，显示如图 8-58 所示的“Setup Type”对话框。在其中选择安装类型。一般选择“Typical”单选按钮即可。

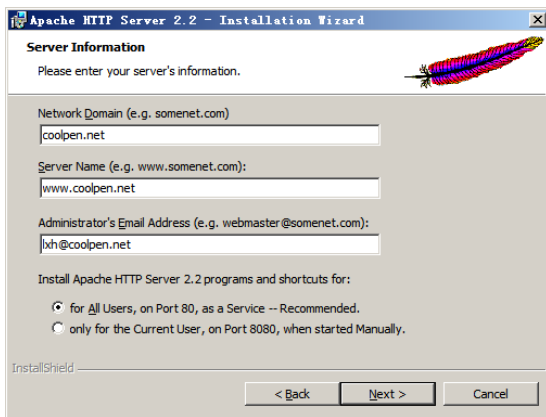


图 8-57 “Server Information”对话框

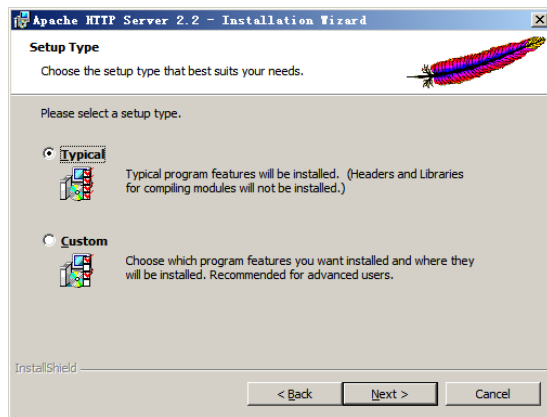


图 8-58 “Setup Type”对话框

⑦ 单击“Next”按钮，显示如图 8-59 所示的“Destination Folder”对话框，在其中设置 Apache 的安装路径。

⑧ 单击“Next”按钮，显示如图 8-60 所示的“Ready to Install the Program”对话框，准备安装 Apache。

⑨ 单击“Install”按钮，开始安装 Apache 程序。安装完成后，显示如图 8-61 所示的 Apache Tomcat 安装完成对话框。

⑩ 单击“Finish”按钮，退出安装向导，Apache 正常运行，在桌面任务栏托盘区域显示一个图标。如果该图标显示为绿色，说明 Apache 正在运行；如果显示为红色，则说明没有运行。右击该图标并选择快捷菜单中的“Open Apache Monitor”选项，显示如图 8-62 所示的“Apache Services Monitor”对话框，可以控制 Apache 服务。

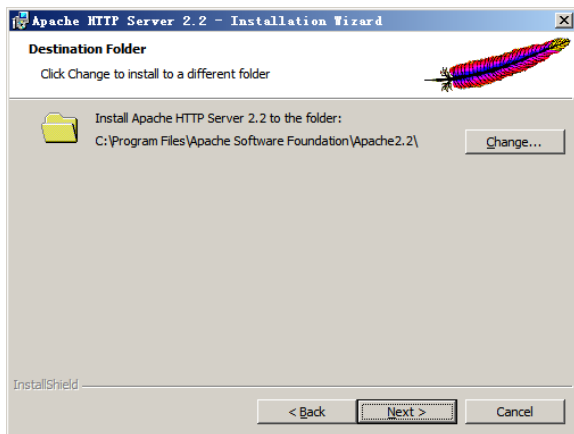


图 8-59 “Destination Folder” 对话框

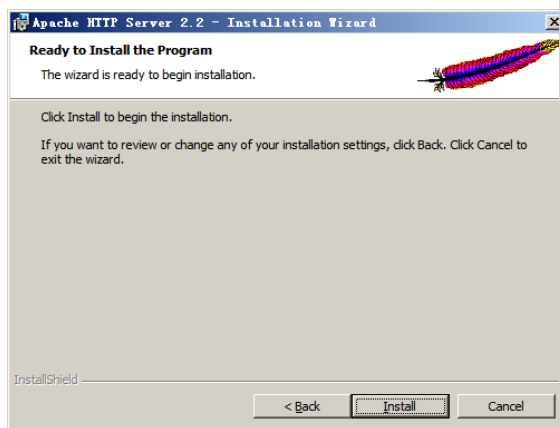


图 8-60 “Ready to Install the Program” 对话框

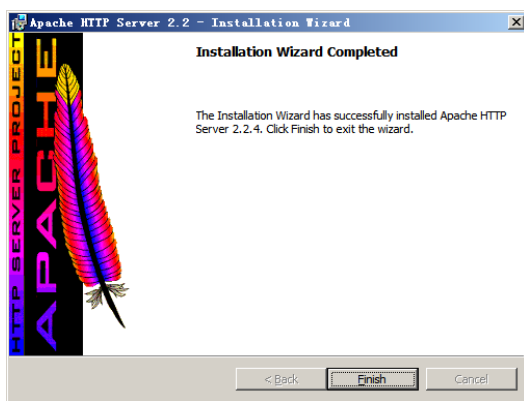


图 8-61 安装完成对话框

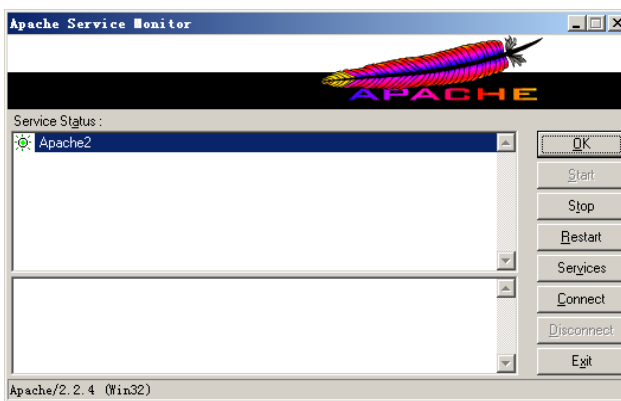


图 8-62 “Apache Services Monitor” 对话框

Apache 安装完成以后，打开 IE 浏览器。在地址栏中输入 Apache 服务器的 IP 地址后按回车键，如果显示如图 8-63 所示的界面，说明 Apache 安装成功并正常运行。

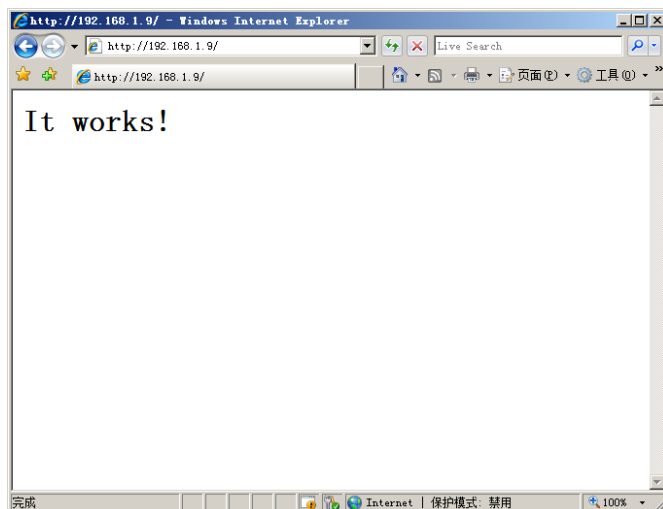


图 8-63 Apache 安装成功并正常运行

8.5.2 配置 Apache

和 IIS 不同，Apache 没有图形界面，因此所有的设置都需要通过修改配置文件的代码来实现。Apache 的配置文件为 httpd.conf，位于 Apache 安装目录（默认为 C:\Program Files\Apache Software

Foundation\Apache2.2\conf) 中。可使用记事本等文本编辑软件打开并编辑, 完成后需要重新启动 Apache 才能使配置生效。

1. 设置域名和端口

在安装 Apache 安装过程中已经设置了 Web 服务器的 DNS 域名, 如果需要更改, 可通过更改“httpd.conf”文件中的 ServerName 来实现。

① 用记事本打开“httpd.conf”文件, 找到“ServerName”。该代码后面的字段就是域名和端口, 这里为 www.coolpen.net:80, 如图 8-64 所示。其中域名为 www.coolpen.net, 端口为 80。如果要更改域名和端口, 只需更改该字段即可。

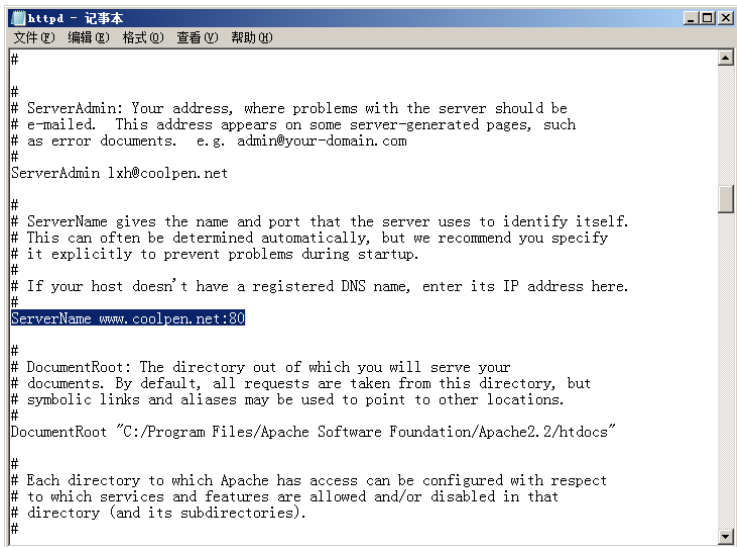


图 8-64 设置域名和端口

② 更改完成后保存即可。

2. 设置根目录

Apache 的根目录默认为安装目录下的“htdocs”文件夹, 为了 Web 服务器的稳定和安全, 应将根目录指定为非系统分区。

① 在“httpd.conf”文件中找到“DocumentRoot”, 该代码后面的字段就是 Web 服务器的默认根目录, 如图 8-65 所示。将此两段代码的路径更改为其他路径即可, 例如“D:\Web”。

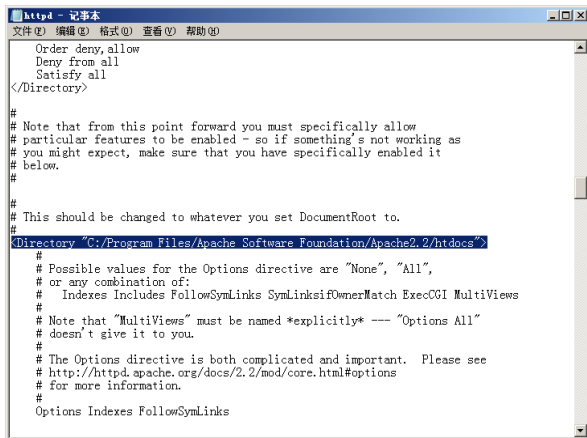
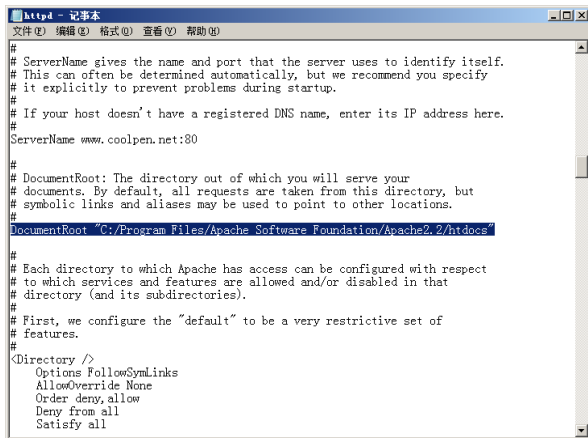


图 8-65 默认根目录

② 设置完成后保存即可。

3. 设置默认文档

默认情况下, Apache 的默认文档为“index.html”。如果要修改或者添加默认文档, 可在“httpd.conf”配置文件中找到“DirectoryIndex”。该代码后面的字段就是默认文档名称, 如图 8-66 所示。如果要添加多个默认文档, 可直接在其后面添加, 多个默认文档之后需要用空格隔开。

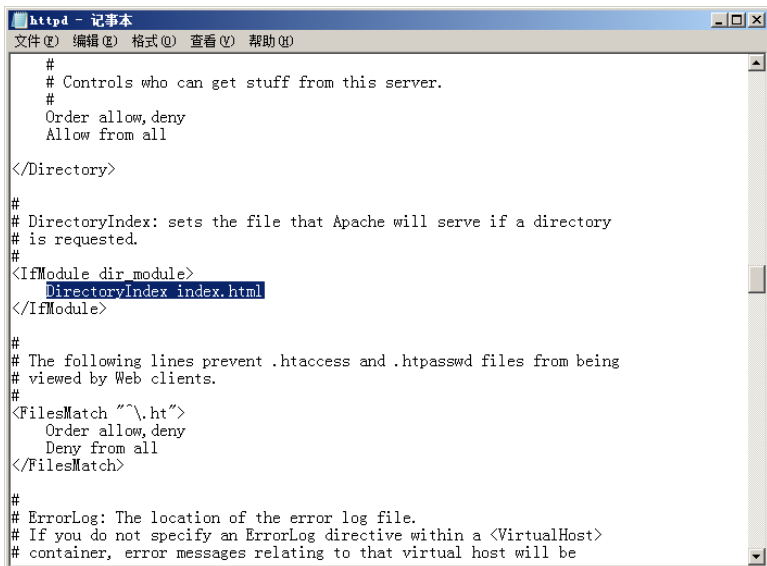


图 8-66 默认文档名称

提示 和 IIS 一样, Apache 在调用默认文档时, 也是按照先后顺序首先调用第 1 个。如果不存在, 则调用第 2 个。依此类推, 因此应将使用的文档放在最前面。

8.6 搭建动态网站环境

默认情况下, IIS 只支持在 Web 网站运行静态 HTML 网页, 但静态网页无法根据用户的需求和实际情况做出相应的变化。因此需要搭建动态网站, 自动接收用户的请求信息并做出反应, 无须人工参与网页的反应即可满足应用需要。搭建动态网站需要部署相应的应用程序, IIS 支持运行多种应用程序。可搭建多种动态网站的运行环境, 如 JSP、CGI、ASP 和 PHP 等。

8.6.1 搭建 JSP 环境

1. JSP 技术简介

JSP (JavaServer Pages) 是由 Sun Microsystems 公司倡导, 由多家公司一起参与并建立的一种动态网页技术标准。JSP 技术与 ASP 技术很相似, 该技术主要使用 JSP 文件, 而 JSP 文件则是在传统的 HTML 网页文件中插入 Java 程序段和 JSP 标记所组成的。

用 JSP 技术开发的 Web 应用程序可以跨平台使用, 即不但可以在 Windows 系统中运行, 还可以在 Linux 系统中运行, 也能在其他操作系统中运行。

JSP 技术主要使用 Java 编程语言编写类 XML 的 tags 和 scriptlets, 并用其来封装产生动态网页的处理逻辑, 使动态网页可以访问服务器端的资源。使用该技术可以将网页逻辑和网页设计分离, 使基于 Web 的应用程序的开发变得更加迅速和容易。

在 Web 服务器上, 当客户端访问的请求中在 JSP 网页时, Web 服务器首先执行网页中的程序段, 然后将 JSP 网页中的 HTML 代码与执行结果一同返回给请求客户端。而此时在客户端所得到的结果往

往只是一个 HTML 文本，因此客户端只要拥有 IE 浏览器即可。需要注意的是，在 JSP 网页中的程序段可以是操作数据库，也可以是重定向的网页等。

2. JSP 的优缺点

JSP 技术具有以下优点。

- (1) 一次编写，处处运行：使用 JSP 技术，除了系统之外，代码不用做任何修改。
- (2) 支持多操作系统平台：JSP 技术基本上可以在所有操作系统上的任意环境中开发，可以在任意环境中进行系统部署，可以在任意环境中进行扩展。
- (3) 强大的可伸缩性：无论是从运行 Servlet/JSP 的 Jar 文件，还是由多台服务器进行集群和负载均衡，或者多台 Application 进行事务和消息处理都显示了 Java 强大的可伸缩性。
- (4) 多样化和功能强大的开发工具支持：目前有很多优秀的 Java 开发工具都是免费提供的，并且这些工具全部可以顺利地运行于多种平台下。

JSP 技术的缺点如下。

- (1) 由于 Java 为了提高跨平台的功能和极度的伸缩能力，因而也极大地增加了产品的复杂性。
- (2) Java 的运行速度是用 class 常驻内存来完成的，因此对内存的要求很严格。另外，Java 还需要大量的硬盘空间来存储一系列的 .java 和 .class 文件，以及对应的版本文件。

3. 安装 Java 开发工具包

Java 开发工具包用来执行 Tomcat 的主程序，而 Tomcat 主程序则用来支持 JSP 运行。Java 开发工具包可以从其官方网站 (<http://java.sun.com/products/archive/index.html>) 下载，也可以从国内一些站点，如天空软件站 (<http://www.skycn.com>) 等网站下载，下载后需要安装。安装过程非常简单，只要接受许可协议，连续单击“下一步”按钮即可。安装完成以后，还需要设置环境变量。

- ① 单击“开始”→“控制面板”→“系统”选项，显示如图 8-67 所示的“系统”窗口。



图 8-67 “系统”窗口

- ② 单击“高级系统设置”链接，打开“系统属性”对话框。打开“高级”选项卡，如图 8-68 所示。

- ③ 单击“环境变量”按钮，显示如图 8-69 所示的“环境变量”对话框，在其中可以修改系统的环境变量。

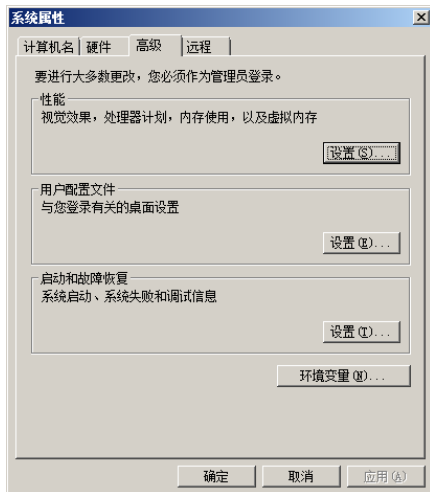


图 8-68 “高级”选项卡

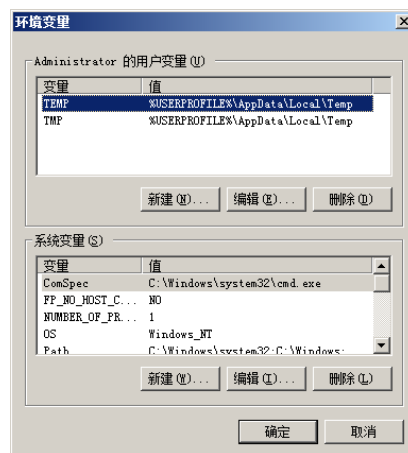


图 8-69 “环境变量”对话框

- ④ 在“系统变量”选项组中单击“新建”按钮，显示如图 8-70 所示的“新建系统变量”对话框。

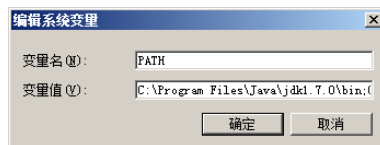


图 8-70 “新建系统变量”对话框

- ⑤ 分别添加表 8-1 所示的环境变量。

表 8-1 环境变量

变 量 名	变量值 (value)
PATH	C:\Program Files\Java\jdk1.7.0\bin;C:\Program Files\Java\jre1.7.0\bin
CLASSPATH	C:\Program Files\Java\jdk1.7.0\lib\dt.jar;C:\Program Files\Java\jdk1.7.0\lib\tools.jar;C:\Program Files\Java\jre1.7.0\lib\rt.jar
JAVA_HOME	C:\Program Files\Java\jdk1.7.0

注：JDK 的安装路径为 C:\Program Files\Java\jdk1.7.0\。

JRE 的安装路径为 C:\Program Files\Java\jre1.7.0\。

- ⑥ 单击“确定”按钮关闭“环境变量”对话框，然后打开命令提示符窗口，分别执行 javac 和 java 命令。如果显示相关命令帮助提示，则表示正常，说明系统可以运行 Java 程序，如图 8-71 所示；否则说明 Java 安装不正常，需要重新安装 Java 程序。



图 8-71 运行 javac 命令

此时即可在服务器上安装 Apache 程序来搭建 JSP 网站。

8.6.2 搭建 CGI 环境

CGI 是微软提供的动态网站技术，可以在 Web 服务器上执行非原生的（Native）的应用程序。例如，可以使用 C++、Delphi 或 Visual Basic 编写一个处理 HTML 表格数据的程序。许多的 CGI 应用程序也是使用指令语言编写的，具有很高的移植性，因此经常被用来延伸 Web 服务器的功能。在 Windows Server 2008 中，只需安装支持 CGI 程序的组件即可。

提示

CGI 缺点是占用服务器的资源比较大，因此对硬件要求比较高。

1. 安装 CGI 服务

- ① 在“服务器管理器”窗口中依次展开“角色”→“Web 服务器”选项，如图 8-72 所示。



图 8-72 展开“角色”→“Web 服务器”选项

- ② 在“角色服务”选项区域中单击“添加角色服务”超级链接，显示如图 8-73 所示的“添加角色服务”对话框，选中“CGI”复选框。

- ③ 单击“下一步”按钮直到安装完成，即可将 CGI 组件安装到 Web 服务器中。

2. 添加 CGI 限制

CGI 组件虽然安装成功，但默认情况下 IIS 服务器并不会自动运行 CGI 程序，需要网络管理员设置允许运行 CGI 程序。

- ① 打开“Internet 信息服务 (IIS) 管理器”窗口，选择 Web 服务器名称，显示如图 8-74 所示的 Web 服务器主页。

- ② 双击“ISAPI 和 CGI 限制”图标，显示如图 8-75 所示的“ISAPI 和 CGI 限制”窗口。

- ③ 在“操作”窗格中单击“添加”按钮，显示如图 8-76 所示的“添加 ISAPI 或 CGI 限制”对话框。在“ISAPI 或 CGI 路径”文本框中单击浏览按钮选择 CGI 应用程序，在“描述”文本框中键入描述信息。如果选中“允许执行扩展路径”复选框，则在设置完成后允许立即执行 CGI 程序。

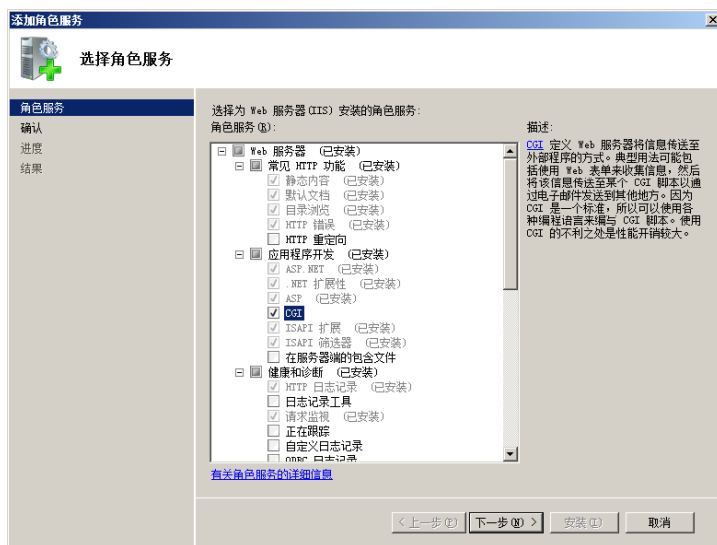


图 8-73 “添加角色服务”对话框



图 8-74 Web 服务器主页



图 8-75 “ISAPI 和 CGI 限制”窗口

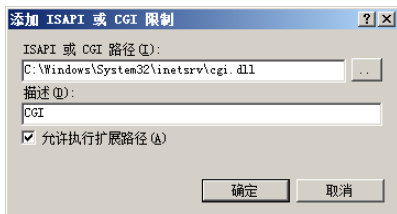


图 8-76 “添加 ISAPI 或 CGI 限制”对话框

- ④ 单击“确定”按钮完成添加，如图 8-77 所示，允许 IIS 执行 CGI 扩展程序。

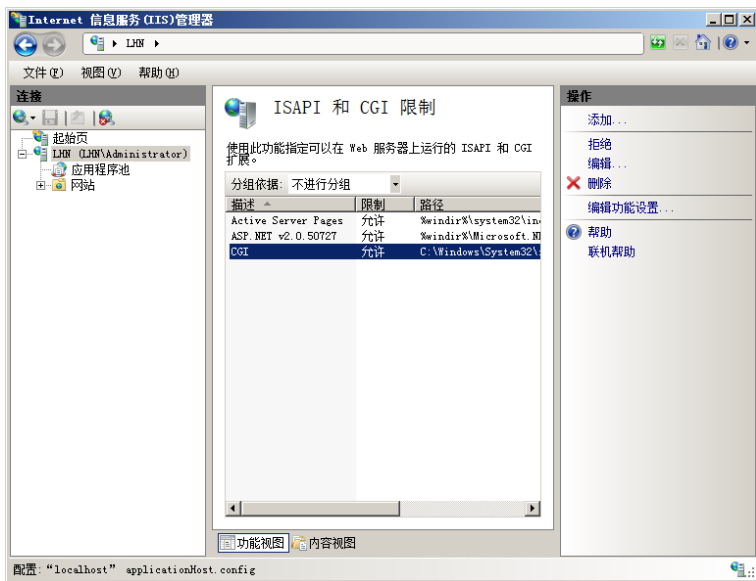


图 8-77 添加 CGI 限制

3. 添加 MIME 类型

默认情况下，Web 服务器并不能识别 CGI 程序，这是因为 Web 服务器的 MIME 类型中并没有“.cgi”。因此需要网络管理员打开如图 8-78 所示的“添加 CGI MIME 类型”对话框后添加，使 Web 服务器可以识别并执行 CGI 程序。



图 8-78 “添加 CGI MIME 类型”对话框

4. 添加 CGI 文件

CGI 程序设置完成以后，用户只需创建一个虚拟目录或者直接将 CGI 程序编写的网页放在主目录文件夹中，即可搭建一个 CGI 网站。当用户访问 CGI 网站时，系统会自动将解释的 CGI 网站返回给用户。

8.6.3 搭建 ASP 环境

Active Server Pages (ASP) 是微软提供的动态网站应用程序，可以用来创建和运行动态交互式网页，充分发挥 IIS 的功能。使用 IIS 架设的 Web 服务器可以使用 HTML 格式撰写 ASP 网页，并使用 Script (VBScript、Jscript 及 JavaScript) 语言来加强 ASP 功能，还可以利用 ODBC 的方式使网页与数

数据库相结合。

1. ASP 和 ASP.NET

ASP 指一种服务器端的脚本运行环境，可用于创建动态交互式网页并建立强大的 Web 应用程序。当 Web 服务器收到对 ASP 文件的请求时会处理服务器端脚本代码，并动态生成相关 Web 页面，自动对用户的请求信息做出反应。ASP 可以与数据库结合使用，数据库中的数据可以随时变化。而服务器中执行的应用程序却不必更改，使客户端可以得到动态更新的网页。除服务器端脚本代码外，ASP 文件也可以包含 HTML（包括相关的客户端脚本）和 COM 组件调用，从而执行不同任务（如连接到数据库或处理商业规则）。

ASP.NET 是 ASP 的下一代升级产品，但提供了为建立和部署企业级 Web 应用程序所必需的服务。它提供了全新编程模型的网络应用程序，能够创建更安全、更稳定且更强大的应用程序。ASP.NET 在语法上与 ASP 基本兼容，并提供了一个新的编程模型和基础架构，用于创建具有更高安全性、可伸缩性和稳定性的应用程序。

ASP.NET 作为 .NET Framework 的一部分，是一个已编译且基于 .NET 的环境，可以使用任何与 .NET 兼容的语言（包括 Visual Basic .NET、C# 和 Jscript .NET）编写应用程序，从而在高度分布的 Internet 环境中简化应用程序开发的计算环境。另外，.NET Framework 还包括可管理的公共语言运行库环境、类型安全和继承功能，在任何 ASP.NET 应用程序中都可以使用这些功能。



提示

.NET Framework 是一个新的计算平台，简化了在 Internet 分布式环境中的应用程序开发过程。其设计宗旨在于提供一种面向对象的编程环境，以确保代码的安全执行，并消除脚本环境中的性能问题。

2. 安装 ASP 服务组件

为了保护 Web 服务器的安全，默认情况下不会自动安装 ASP 服务组件，需要网络管理员手动安装。

在“添加角色服务”向导中选中“ASP.NET”和“ASP”复选框即可安装 ASP.NET 和 ASP 服务，如图 8-79 所示。

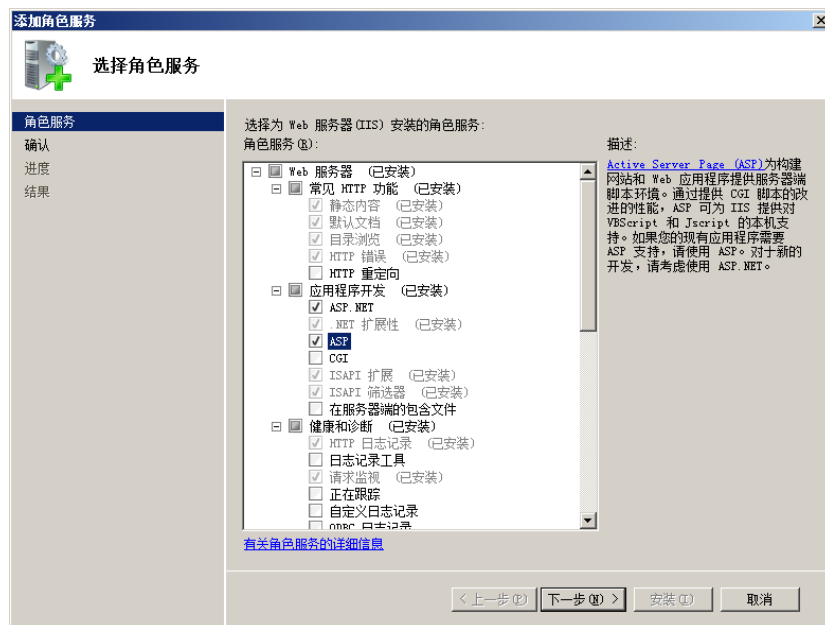


图 8-79 安装 ASP.NET 和 ASP 服务

3. 设置 ASP

打开 IIS 管理器，选择 Web 网站。在主页窗口中双击“ASP”图标，显示如图 8-80 所示的“ASP”窗口。在其中可以设置 ASP 的属性，包括编译、服务和行为等。

当用户发布 ASP 网页时，只需将已制作的 ASP 网页放入 Web 网站的主目录中即可，其他用户即可直接访问该 Web 网站的 ASP 网页。

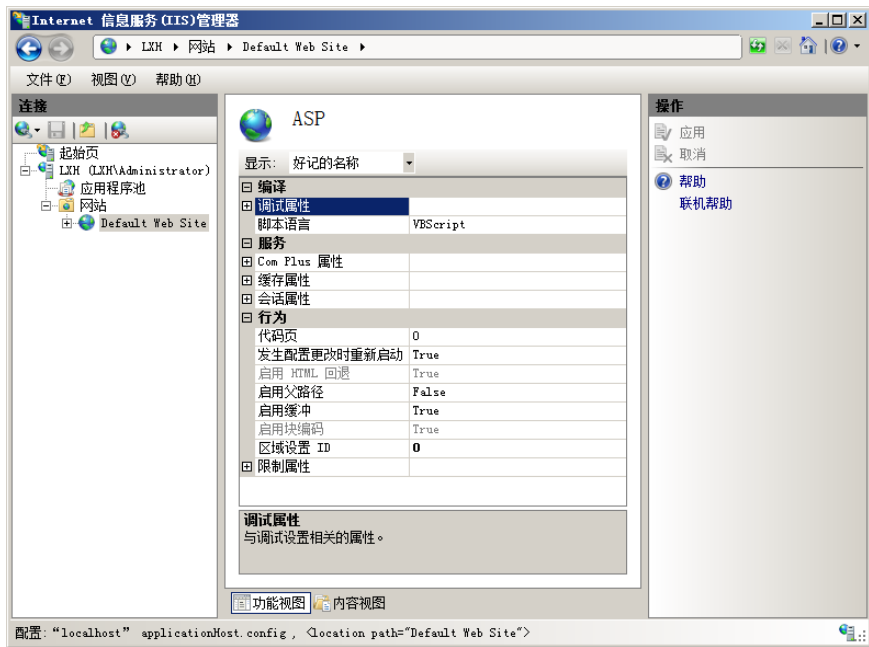


图 8-80 “ASP”窗口

8.6.4 搭建 PHP 环境

PHP 是一种新型的 CGI 程序编写语言，易学易用且运行速度快，用其可以方便快捷地编写出功能强大、运行速度快，并可同时运行于 Windows、Unix 及 Linux 操作系统的 Web 程序。PHP 内置了文件上传、密码认证、Cookies 操作、邮件收发及动态 GIF 生成等功能，并直接为很多数据库提供原本的连接，包括 Oracle、Sybase、Postgres、Mysql、Informix、Dbase、Solid 及 Access 等。它完全支持 ODBC 接口，用户更换平台时无须变换 PHP 代码即可使用。

1. 软件准备

默认情况下，IIS 7.0 不支持 PHP 程序，需要手动安装 PHP 程序。另外，PHP 程序需要 mysql 的支持。PHP 当前 for Windows 的最新版本为 PHP v5.2 版，支持 Windows 9x/Me/NT/2000/XP/2003/2008 等系统。可以从其官方网站（<http://www.php.net/>）下载，也可以从国内一些站点，如天空软件站（<http://www.skycn.com/>）等下载。

① 运行 PHP 安装程序，显示如图 8-81 所示的安装向导。

② 单击“Next”按钮，显示如图 8-82 所示的“End-User License Agreement”对话框，提示需要阅读并接受最终用户许可协议。选中“I accept the terms in the License Agreement”复选框，接受许可协议。

③ 单击“Next”按钮，显示如图 8-83 所示的“Destination Folder”对话框，在其中设置 PHP 程序的安装路径。

④ 单击“Next”按钮，显示如图 8-84 所示的“Web Server Setup”对话框。在其中选择待安装的 Web 服务器类型，这里选择“IIS ISAPI module”单选按钮，安装 IIS ISAPI 模块。

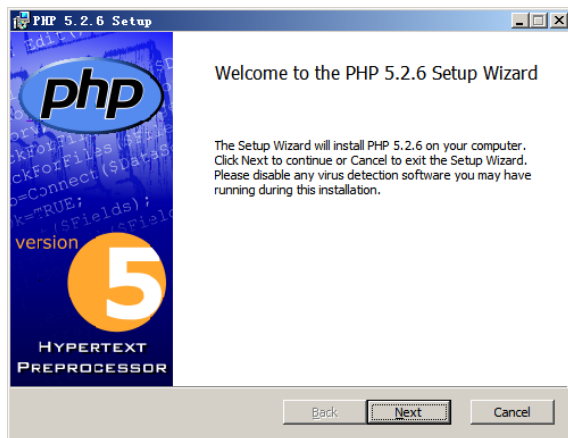


图 8-81 PHP 安装向导

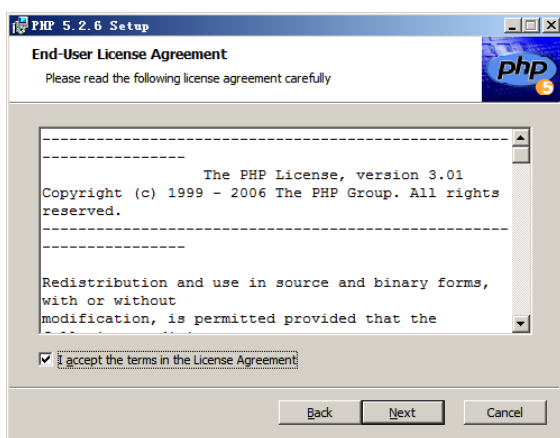


图 8-82 “End-User License Agreement” 对话框

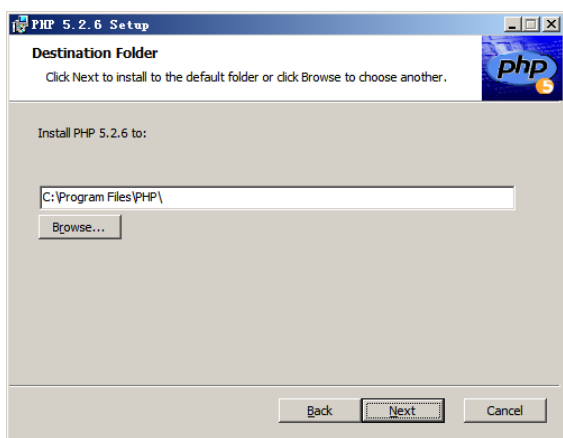


图 8-83 “Destination Folder” 对话框

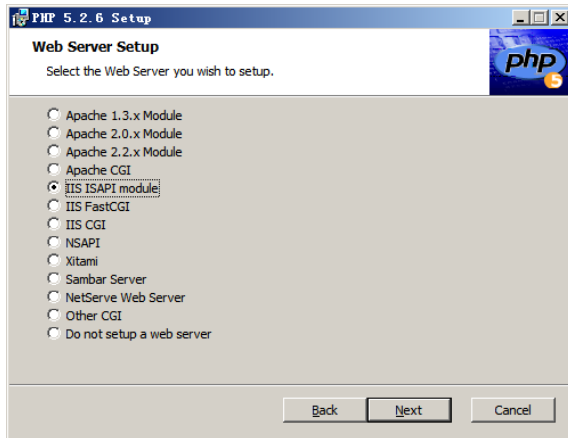


图 8-84 “Web Server Setup” 对话框

⑤ 单击“Next”按钮，显示如图 8-85 所示的“Choose Items to Install”对话框。在列表框中可选择待安装的组件，使用默认设置即可。

⑥ 单击“Next”按钮，显示如图 8-86 所示的“Ready to install PHP 5.2.6”对话框，提示将要开始安装 PHP。

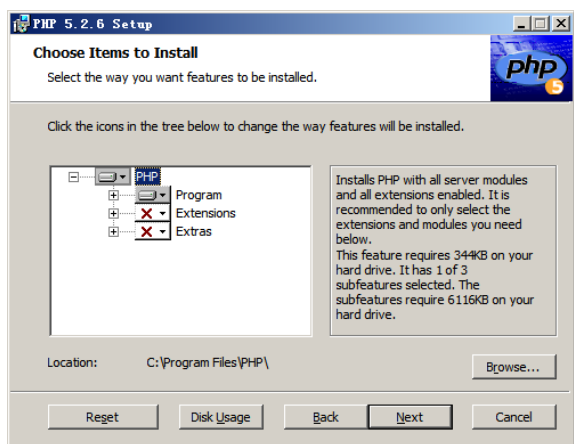


图 8-85 “Choose Items to Install” 对话框

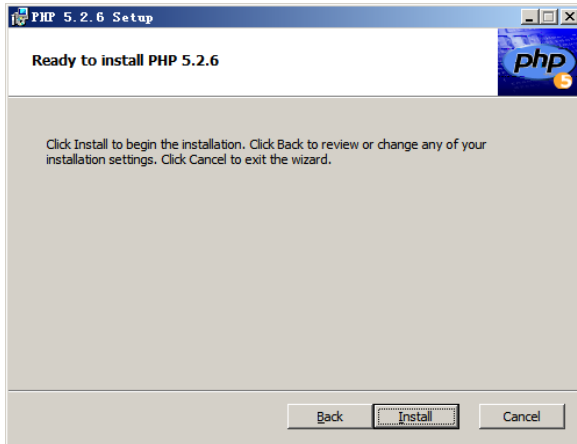


图 8-86 “Ready to install PHP 5.2.6” 对话框

⑦ 单击“Next”按钮，显示如图 8-87 所示的“Completed the PHP 5.2.6 Setup Wizard”对话框，提示 PHP 已安装完成。

- ⑧ 单击“Finish”按钮，完成 PHP 的安装。

2. 配置 PHP

① 打开 IIS 管理器窗口，在网站设置主页中双击“ISAPI 筛选器”图标，打开“ISAPI 筛选器”窗口。在右侧“操作”窗格中单击“添加”按钮，显示如图 8-88 所示的“添加 ISAPI 筛选器”对话框。在“筛选器名称”文本框中键入名称 php，单击“可执行文件”文本框的浏览按钮，选择 Php 安装目录中的 php5isapi.dll 文件。设置完成后，单击“确定”按钮保存设置。



图 8-87 “Completed the PHP 5.2.6 Setup Wizard”对话框

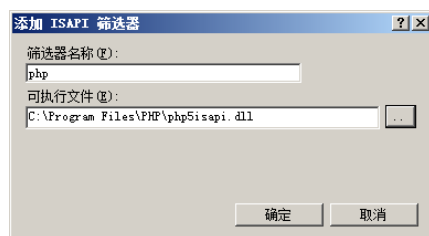


图 8-88 “添加 ISAPI 筛选器”对话框

② 为添加脚本映射，在网站设置主页中双击“处理程序映射”图标打开“处理程序映射”窗口，如图 8-89 所示。

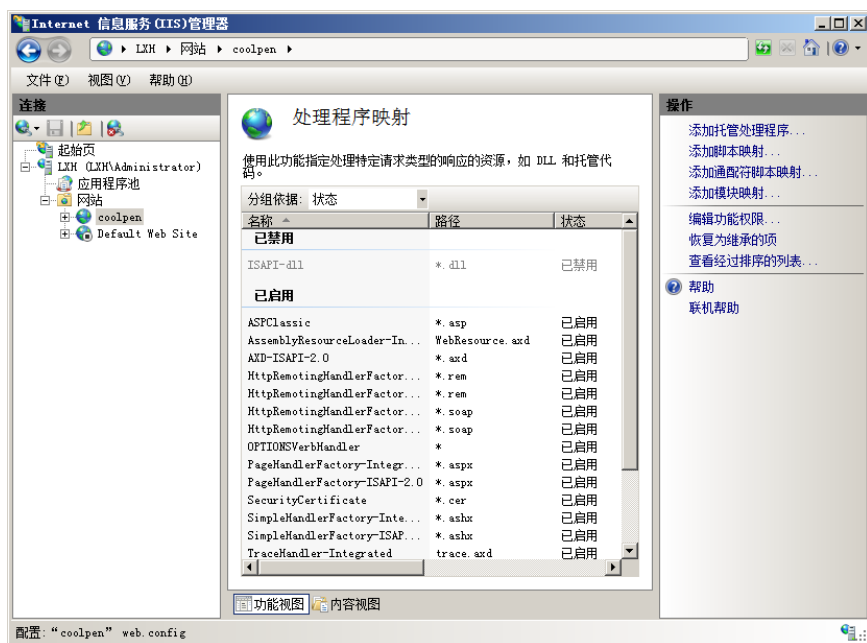


图 8-89 “处理程序映射”窗口

③ 在右侧“操作”窗格中单击“添加脚本映射”按钮，显示如图 8-90 所示的“添加脚本映射”对话框。在“请求路径”文本框中键入*.php，单击“可执行文件”文本框的浏览按钮选择 php 安装目录中的 php5isapi.dll 文件，在“名称”文本框中键入 php。

④ 完成后单击“确定”按钮，显示如图 8-91 所示的“添加脚本映射”对话框，单击“是”按钮即可。



图 8-90 “添加脚本映射”对话框

⑤ 为添加应用程序池，在“Internet 信息服务 (IIS) 管理器”窗口的右侧窗格中选择“应用程序池”选项。然后在“应用程序池”窗口中右侧“操作”窗格中单击“添加应用程序池”按钮，显示如图 8-92 所示的“添加应用程序池”对话框。

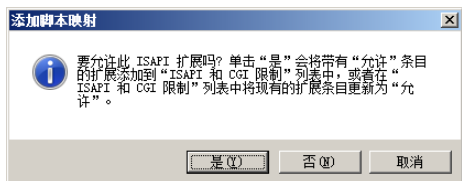


图 8-91 “添加脚本映射”对话框

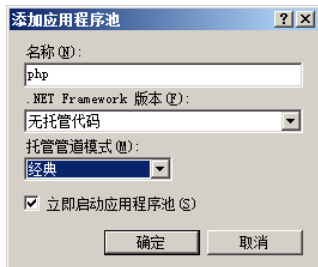


图 8-92 “添加应用程序池”对话框

设置如下选项。

- 名称：在该文本框中键入 php。
- .NET Framework 版本：在其中选择“无托管代码”选项。
- 托管管道模式：在其中选择“经典”选项。
- 立即启动应用程序池：选中该复选框，可以在设置完成后立即启动该应用程序池。

⑥ 单击“确定”按钮保存设置。

⑦ 添加名为“index.php”的默认文档，操作步骤请参见前面相关的内容，这里不再赘述。

至此，PHP 环境已经搭建完成，下面在网站主目录中创建一个测试页，检查该环境是否能够正常运行。

在网站主目录中新建一个 index.php 文件，键入如下文件内容：

```
<?php
Phpinfo();
?>
```

保存并退出。

⑧ 打开 IE 浏览器，在地址栏中键入网站的主机名。按回车键，显示如图 8-93 所示的 Web 服务器的 PHP 测试页。

8.7 安装与设置数据库

动态网站通常都要使用数据库存储数据，例如一些 BBS 论坛等往往保存了大量的用户数据。目前使用最多的是 SQL（结构化查询语言）和 Access 数据库，而 SQL 数据库 MySQL 因其短小、易用且免费等特点，赢得了广大用户的喜爱。

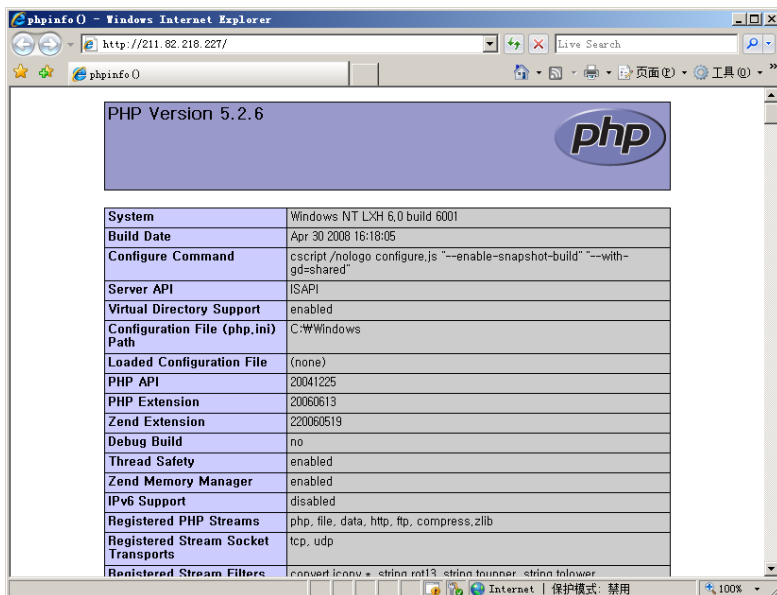


图 8-93 PHP 测试页

8.7.1 安装与设置 MySQL

MySQL 是 SQL 语言中的一种，它提供 SQL 的后台数据库。尤其是当前台使用 PHP 和 CGI 语言时，能够提供最好的支持。为了充分发挥 PHP 的优势，应在 Web 服务器上安装 MySQL 数据库。

MySQL 是一个免费软件，用户可以从其官方网站（<http://www.mysql.com/>）或国内的站点下载。MySQL 的安装也非常简单，只需连续单击“Next”按钮即可，安装完成后即可使用。

① 安装完成 MySQL 后会自动运行配置向导，如图 8-94 所示。也可以单击“开始”→“所有程序”→“MySQL”→“MySQL Server 5.0”→“MySQL Server Instance Configuration Wizard”选项来启动该向导。

② 单击“Next”按钮，显示 MySQL 配置向导之一，选择配置类型，如图 8-95 所示。这里，选择“Detailed Configuration”（详细配置）单选按钮。

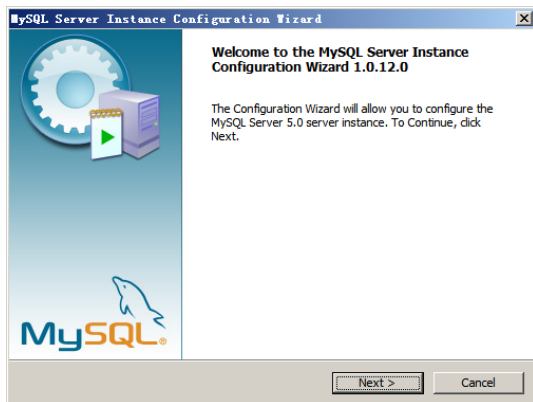


图 8-94 MySQL 配置向导

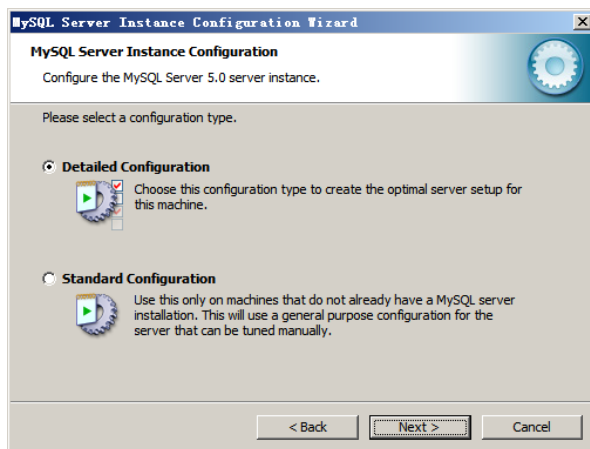


图 8-95 选择配置类型

③ 单击“Next”按钮，显示 MySQL 配置向导之二。选择服务器类型，如图 8-96 所示，这里选择“Server Machine”单选按钮。

④ 单击“Next”按钮，显示 MySQL 配置向导之三。选择数据库类型，如图 8-97 所示，这里选择“Multifunctional Database”单选按钮。

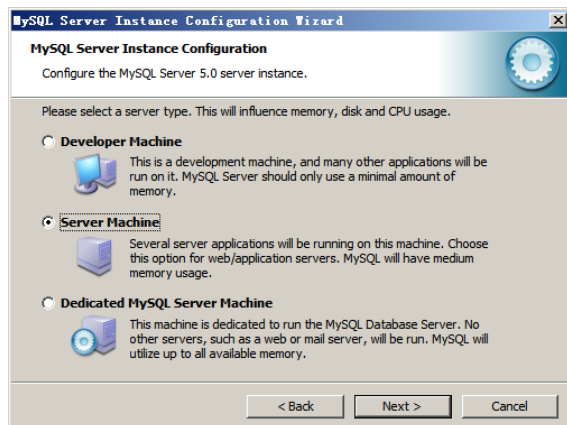


图 8-96 选择服务器类型

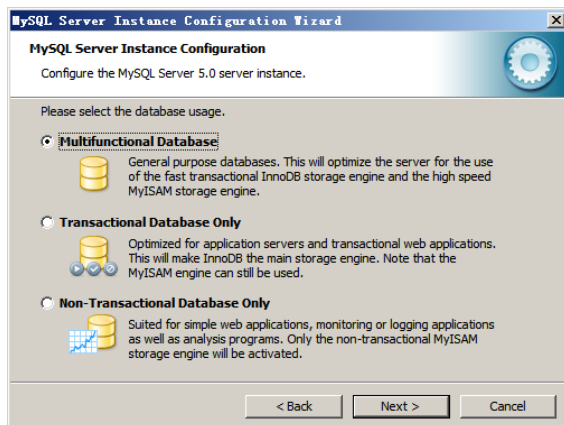


图 8-97 选择数据库类型

⑤ 单击“Next”按钮，显示 MySQL 配置向导之四。设置安装路径，如图 8-98 所示。

⑥ 单击“Next”按钮，显示 MySQL 配置向导之五。设置服务器的并发连接数量，如图 8-99 所示。

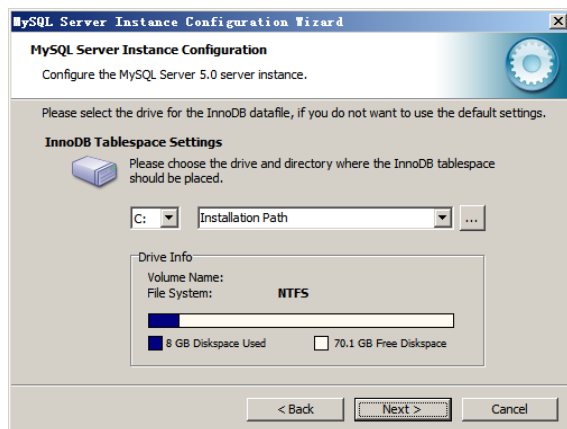


图 8-98 选择安装路径

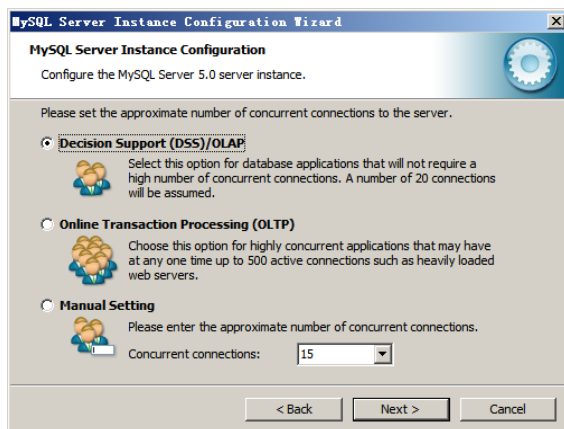


图 8-99 设置服务器的并发连接数量

⑦ 单击“Next”按钮，显示 MySQL 配置向导之六。设置 MySQL 服务的网络选项。通常使用默认设置，即启用 TCP/IP 网络连接方式，如图 8-100 所示。

⑧ 单击“Next”按钮，显示 MySQL 配置向导之七。选择“Standard Character Set”单选按钮，使用标准字符设置，如图 8-101 所示。

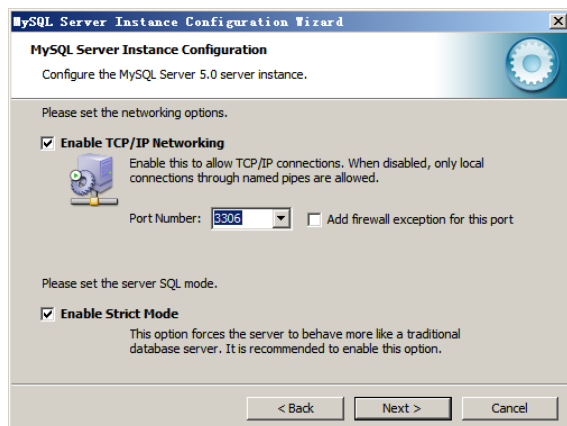


图 8-100 设置网络选项

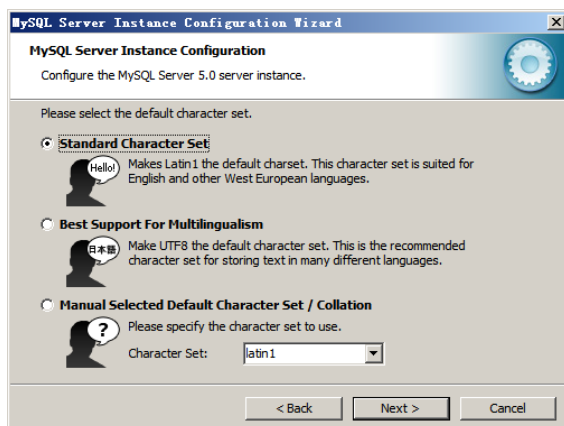


图 8-101 选择“Standard Character Set”单选按钮

⑨ 单击“Next”按钮，显示 MySQL 配置向导之八。选中“Install As Windows Service”复选框，并在“Service Name”下拉列表框中选择 MySQL 的服务名称。将 MySQL 设置为系统服务，如图 8-102 所示。

⑩ 单击“Next”按钮，显示 MySQL 配置向导之九。选中“Modify Security Settings”复选框，分别在“New root password”和“Confirm”文本框中为 MySQL 设置一个登录密码，如图 8-103 所示。



图 8-102 设置系统服务

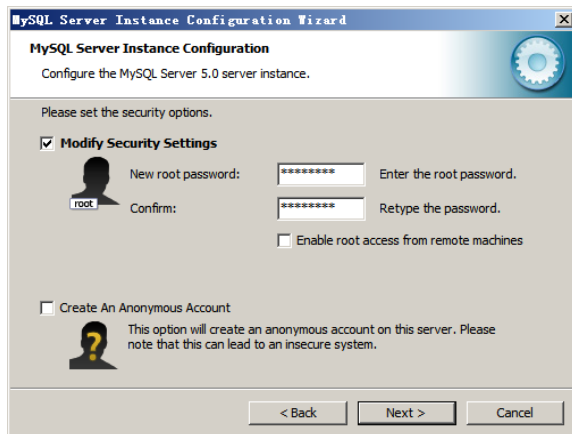


图 8-103 设置安全选项

⑪ 单击“Next”按钮，显示 MySQL 配置向导之十。提示将开始执行 MySQL 配置，如图 8-104 所示。

⑫ 单击“Execute”按钮开始配置 MySQL，如图 8-105 所示，配置完成后单击“Finish”按钮退出即可。

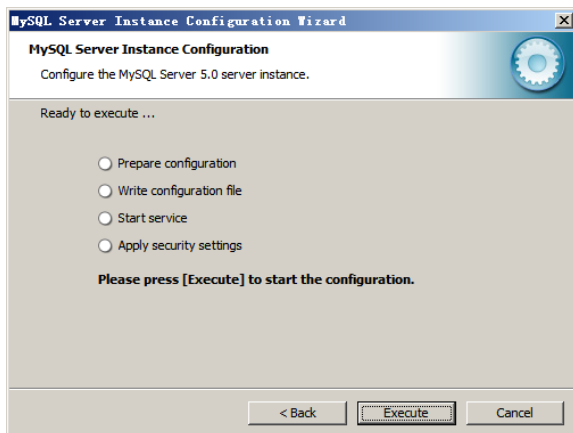


图 8-104 准备执行 MySQL 配置

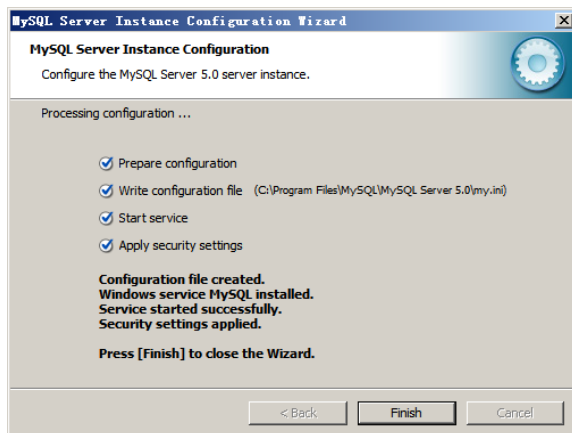


图 8-105 开始配置 MySQL

至此，MySQL 配置已经完成，现在可以将 PHP 与 MySQL 数据库文件配合使用。

8.7.2 安装与设置 SQL Server

Microsoft SQL Server 2005 是微软公司的数据库软件，可为很多应用程序提供数据库支持。对于 Web 服务器来说，SQL Server 2005 可以安装在 Web 服务器或网络中的服务器上，安装过程如下。

① 将 SQL Server 2005 安装光盘放入光驱，打开光盘的“Servers”目录。运行“Setup.exe”程序，显示如图 8-106 所示的“程序兼容性助手”对话框。

② 单击“运行程序”按钮，显示如图 8-107 所示的“最终用户许可协议”对话框，选中“我接受许可条款和条件”复选框。

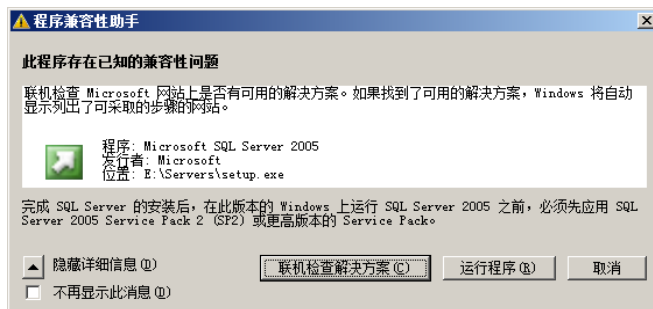


图 8-106 “程序兼容性助手”对话框

③ 单击“下一步”按钮，显示如图 8-108 所示的“安装必备组件”对话框，单击“安装”按钮安装必备组件。

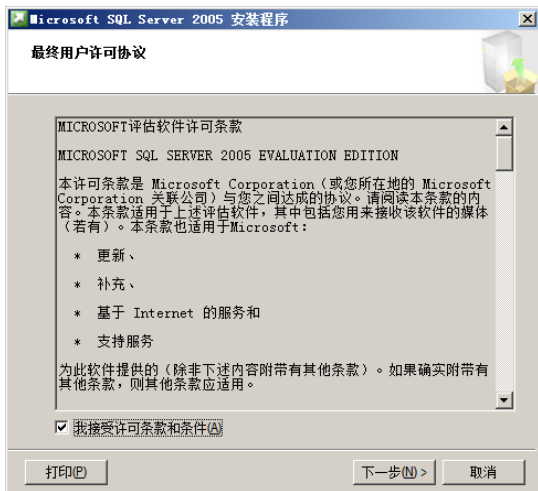


图 8-107 “最终用户许可协议”对话框

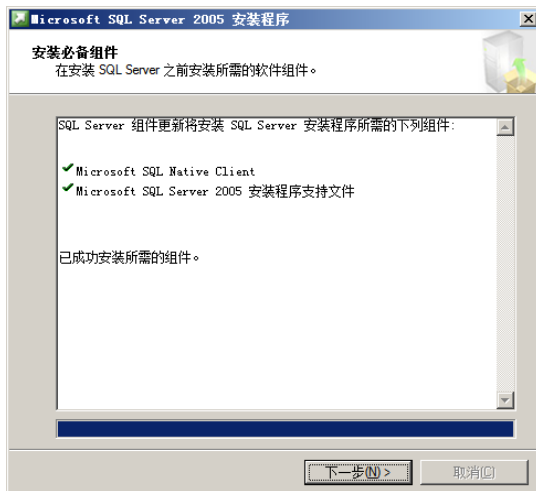


图 8-108 “安装必备组件”对话框

④ 单击“下一步”按钮，开始检查系统配置。完成后启动 Microsoft SQL Server 2005 安装程序向导，如图 8-109 所示。

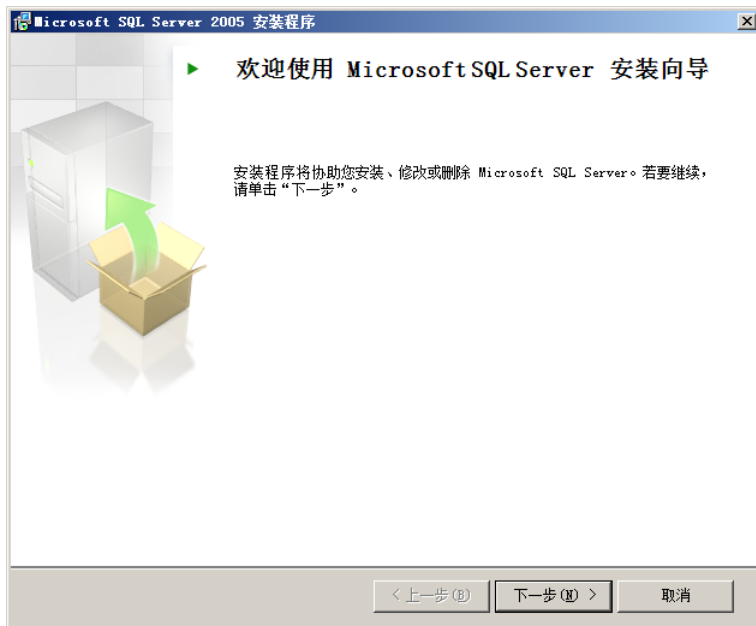


图 8-109 Microsoft SQL Server 2005 安装程序向导

⑤ 单击“下一步”按钮，显示如图 8-110 所示的“系统配置检查”对话框。在“详细信息”列表框中列出了 SQL Server 的安装需求，显示为“成功”的项表示没有安装问题。



图 8-110 “系统配置检查”对话框

⑥ 单击“下一步”按钮，显示如图 8-111 所示的“注册信息”对话框，键入用户的姓名和公司信息。

⑦ 单击“下一步”按钮，显示如图 8-112 所示的“要安装的组件”对话框，选择待安装的组件即可。

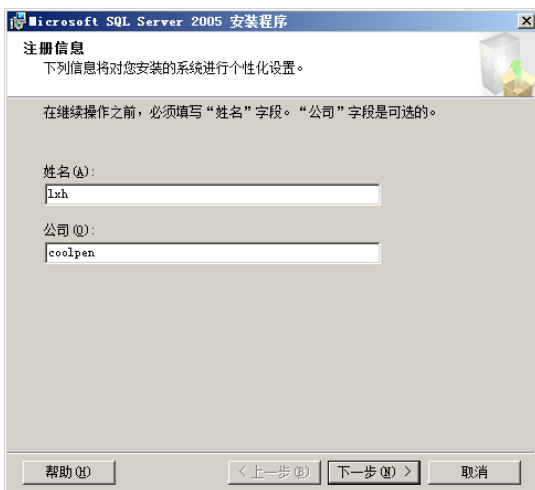


图 8-111 “注册信息”对话框



图 8-112 “要安装的组件”对话框

⑧ 单击“下一步”按钮，显示如图 8-113 所示的“实例名”对话框。在其中选择安装默认实例还是命名实例，默认选择“默认实例”单选按钮。如果需要升级现有命名实例，则单击“命名实例”单选按钮并指定实例名称。

⑨ 单击“下一步”按钮，显示如图 8-114 所示的“服务账户”对话框。在其中选择使用哪种账户登录，可使用系统内置账户，也可以使用域用户账户。在“安装结束时启动服务”选项组中，选择安装完成后要启动的服务。

⑩ 单击“下一步”按钮，显示如图 8-115 所示的“身份验证模式”对话框，在其中选择连接 SQL Server 时要使用的身份验证模式。

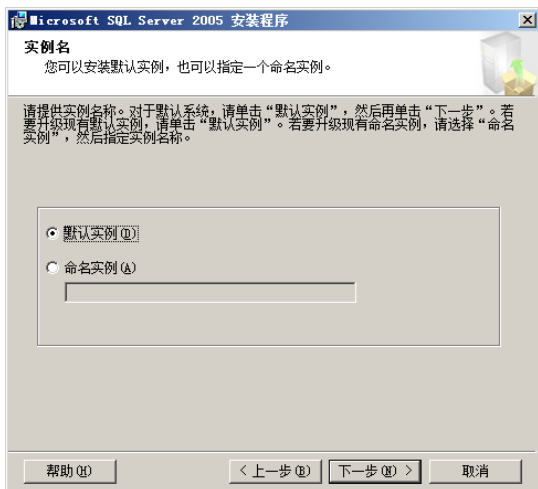


图 8-113 “实例名”对话框



图 8-114 “服务账户”对话框

⑪ 单击“下一步”按钮，显示如图 8-116 所示的“排序规则设置”对话框，在其中设置定义服务器的排序方式。

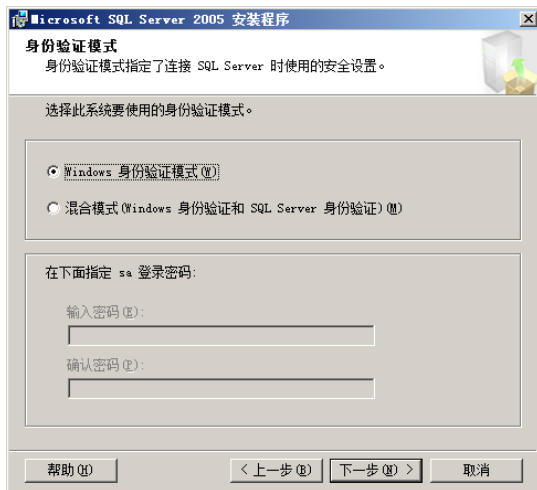


图 8-115 “身份验证模式”对话框

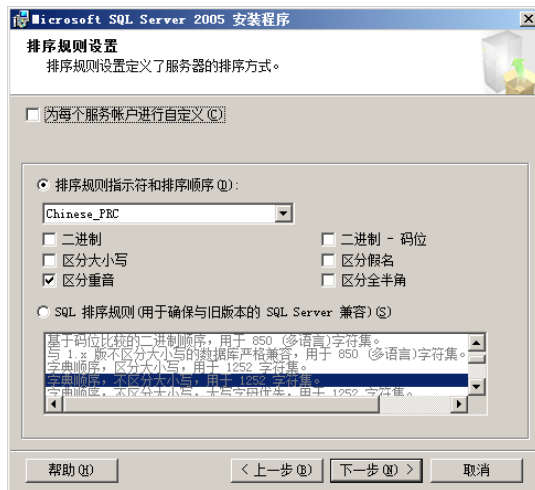


图 8-116 “排序规则设置”对话框

⑫ 单击“下一步”按钮，显示如图 8-117 所示的“错误和使用情况报告设置”对话框，使用默认设置即可。

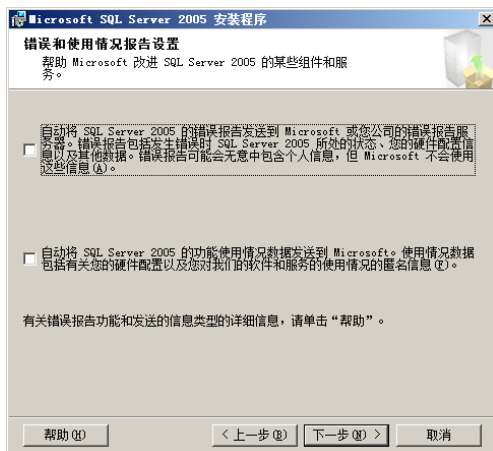


图 8-117 “错误和使用情况报告设置”对话框

⑬ 单击“下一步”按钮，显示如图 8-118 所示的“准备安装”对话框，在“将安装以下组件”列表框中显示将要安装的组件。如果需要更改，则单击“上一步”按钮返回。

⑭ 单击“安装”按钮，开始安装并配置所选择的组件，显示如图 8-119 所示的“安装进度”对话框。该安装过程需要一段时间，请耐心等待。



图 8-118 “准备安装”对话框

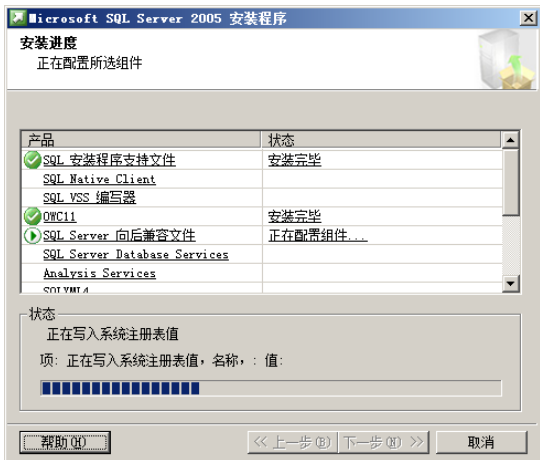


图 8-119 “安装进度”对话框

⑮ 安装完成后，显示如图 8-120 所示的对话框，提示各种组件都已安装完毕。

⑯ 单击“下一步”按钮，显示如图 8-121 所示的“完成 Microsoft SQL Server 2005”对话框，提示已经配置完成 SQL Server 2005。



图 8-120 安装完成



图 8-121 “完成 Microsoft SQL Server 2005”对话框

⑰ 单击“完成”按钮，关闭安装向导。

8.8 Web 网站的远程管理

当网站搭建以后，需要经常对其进行管理。为了便于用户随时可从远程计算机上管理 Web 网站，IIS 7.0 提供了远程管理功能。只要在远程计算机中安装了 IIS 7.0，用户即可连接 Web 服务器并管理 IIS 站点、服务器或者应用程序，而不必坐到服务器面前。在 Windows Server 2008 中连接到目标站点提供连接向导，根据提示即可完成目标站点的连接。

8.8.1 安装管理服务

如果要安装远程管理工具，则在“服务器管理器”窗口中选择 Web 服务器角色。单击“添加角色

服务”超级链接，显示“选择角色服务”对话框。选中“管理服务”复选框，如图 8-122 所示。也可以在安装 Web 服务器过程中选择安装。

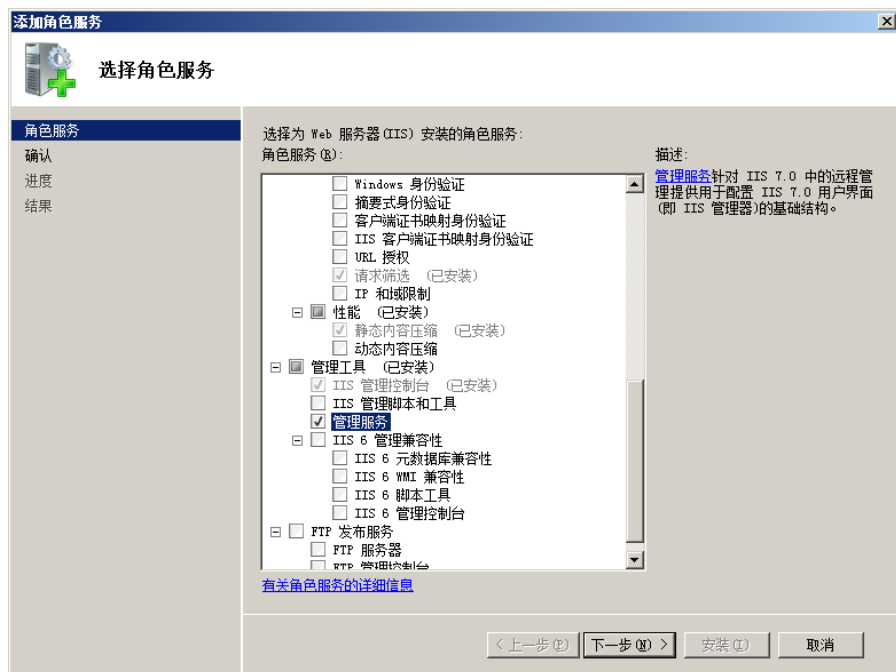


图 8-122 选中“管理服务”复选框

8.8.2 启用远程管理功能

安装完成 IIS 的管理组件以后，默认不允许用户远程管理 Web 服务器。因此需要管理员启用远程连接功能，并指定允许远程管理 IIS 的用户。

① 打开 IIS 管理器窗口，选择 Web 服务器名称。在“主页”窗口中双击“管理”区域的“管理服务”图标，显示如图 8-123 所示的“管理服务”窗口。

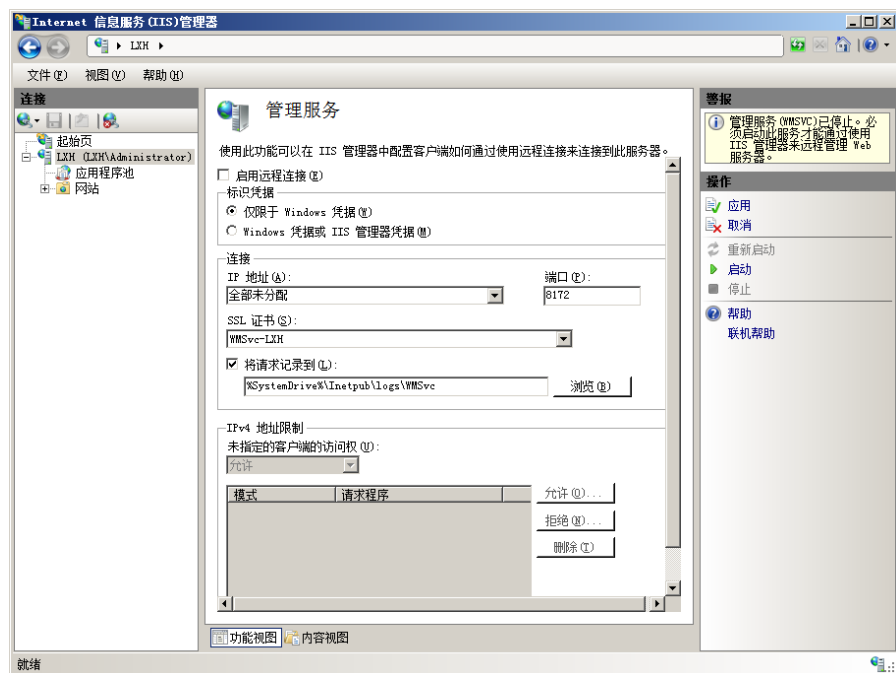


图 8-123 “管理服务”窗口

- ② 选中“启用远程连接”复选框，允许用户远程管理该 Web 服务器，然后设置如下选项：
- 标识凭据：如果仅允许 Windows 身份用户登录，选择“仅限于 Windows 凭据”单选按钮；如果既允许 Windows 用户登录，又允许非 Windows 用户登录（非 IIS 管理员，即临时管理 IIS 服务器的用户），则选择“Windows 凭据或 IIS 管理器凭据”单选按钮。
 - 连接：在“IP 地址”下拉列表框中为 IIS 指定唯一的远程连接 IP 地址，管理端口默认为 8172，在“SSL 证书”下拉列表框中选择远程连接时使用的证书。
 - 将请求记录到：设置记录远程连接请求的日志文件。
 - IPv4 地址限制：添加允许访问 IIS 的用户账户，在“未指定的客户端的访问权”下拉列表框中选择“允许”选项。单击“允许”按钮，显示如图 8-124 所示的“添加允许连接规则”对话框。选择“特定 IPv4 地址”单选按钮，并键入允许访问 IIS 服务器的 IP 地址。如果要键入一个 IP 地址，则选择“IPv4 地址范围”单选按钮，单击“确定”按钮添加。

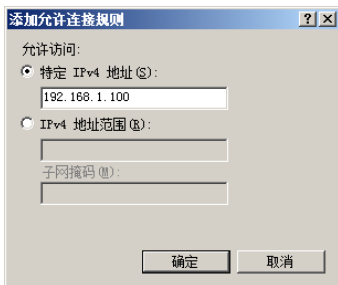


图 8-124 “添加允许连接规则”对话框

- ③ 设置完成后，显示设置的管理服务如图 8-125 所示。在“操作”窗格中单击“应用”按钮保存设置。

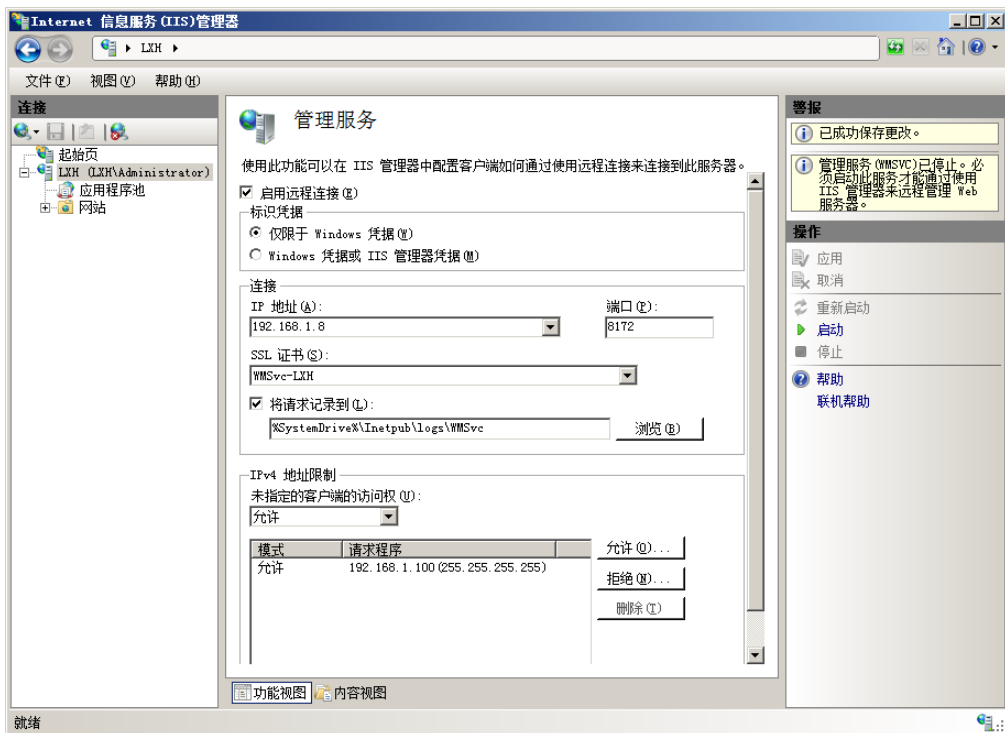


图 8-125 设置的管理服务

- ④ 在“操作”窗格中单击“启动”超级链接，启动管理服务。“管理服务”窗口中的所有设置为“只读”状态，如图 8-126 所示。

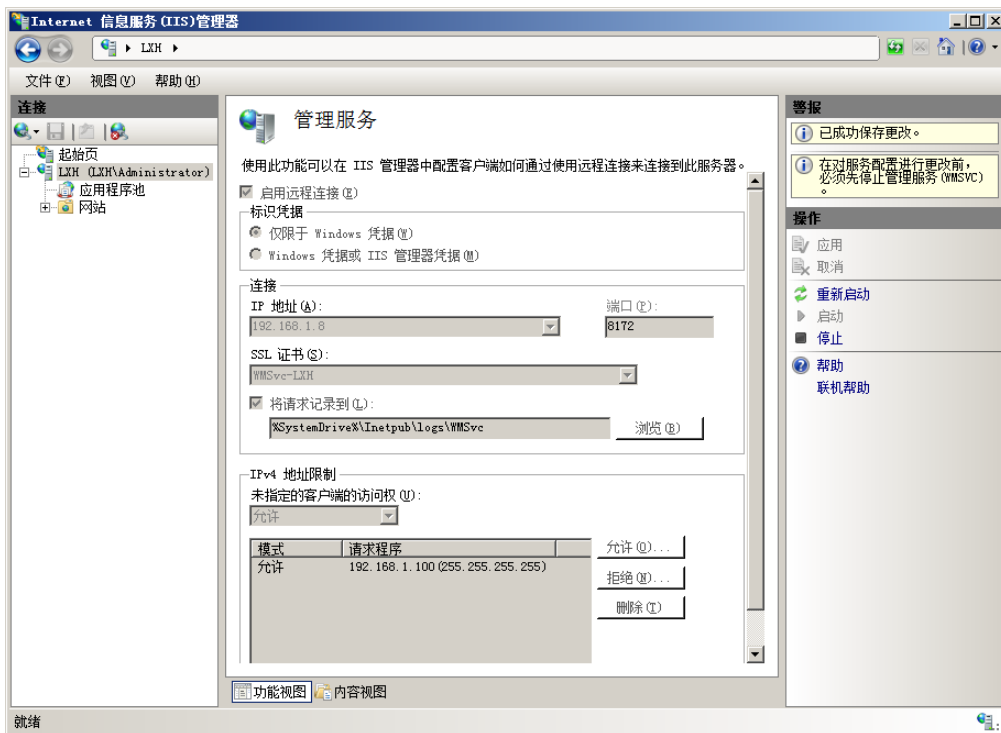


图 8-126 启动管理服务

8.8.3 创建 IIS 管理用户

管理 IIS 的用户可以是 Windows 用户账户，也可以是在 IIS 中创建的非 Windows 用户。不过，Windows 用户可以和 Windows Server 2008 提供的 NTFS 机制更好地融合，而非 Windows 用户则只能应用于临时委托某个用户管理 IIS 站点的环境。

如果仅允许具有 Windows 身份的用户远程管理 IIS，那么需要在系统中创建相应的用户账户，如图 8-127 所示。

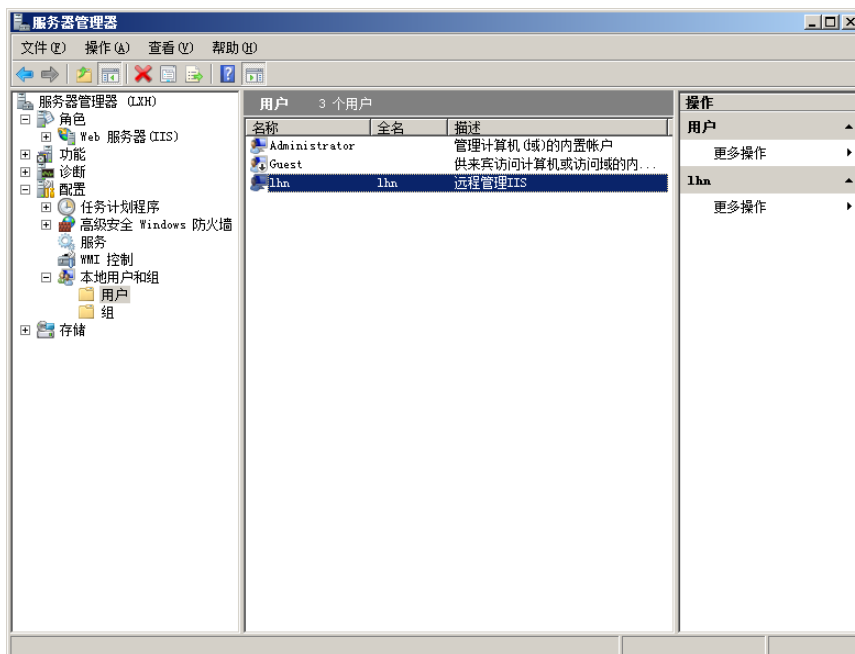


图 8-127 创建 Windows 用户账户

如果要允许非 Windows 用户远程管理 IIS，那么需要在 IIS 中创建临时 IIS 用户。该用户不具有 Windows 权限，只能用于管理 IIS。操作过程如下。

① 打开 IIS 管理器，选择服务器名称。在“主页”窗口中的“管理”选项区域中双击“IIS 管理器用户”图标，显示如图 8-128 所示的“IIS 管理器用户”窗口。

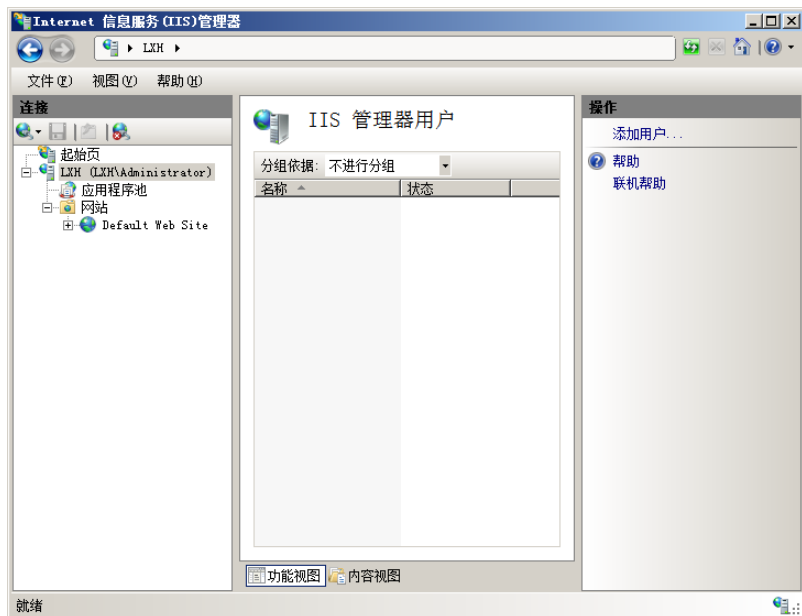


图 8-128 “IIS 管理器用户”窗口

② 在“操作”窗格中单击“添加用户”超级链接，显示如图 8-129 所示的“添加用户”对话框，在“用户名”文本框中键入新用户名，在“密码”文本框中设置用户密码。

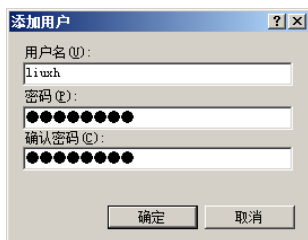


图 8-129 “添加用户”对话框

此处建议使用强密码，即需要满足如下条件。

- 不包含全部或部分的账户名。
- 长度至少为 7 个字符。
- 包含来自以下 4 个类别中的至少 3 个的字符。
 - 英文大写字母 (A~Z)。
 - 英文小写字母 (a~z)。
 - 10 个基本数字 (0~9)。
 - 非字母字符 (例如，!、\$、#及%)。



提示

虽然系统建议使用强密码，但用户仍可设置简单密码。不过为安全起见，建议使用强密码。

③ 单击“确定”按钮，一个 IIS 用户添加完成，如图 8-130 所示。



图 8-130 添加一个 IIS 用户

8.8.4 授权远程管理用户

无论 Windows 用户，还是非 Windows 用户，默认都没有启动管理 IIS 的权限，因此必须由管理员为待远程管理 IIS 的用户授予管理 IIS 权限。要为用户授予管理 IIS 权限，必须在需要管理的 Web 站点中授权。

① 打开 IIS 管理器，选择待添加授权用户的 Web 站点。在“主页”窗口中双击“IIS 管理器权限”图标，显示如图 8-131 所示的“IIS 管理器权限”窗口。



图 8-131 “IIS 管理器权限”窗口

② 在“操作”窗格中单击“允许用户”超级链接，显示如图 8-132 所示的“允许用户”对话框。如果为该 Web 站点选择 Windows 用户，则选择“Windows”单选按钮。并键入用户名，或者单击“选择”按钮从系统中选择。

如果要使用非 Windows 用户管理 Web 站点，则选择“IIS 管理器”单选按钮。并键入非 Windows 用户名，如图 8-133 所示，也可以单击“选择”按钮选择。

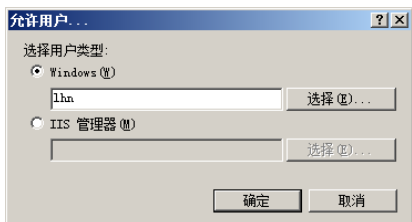


图 8-132 “允许用户”对话框

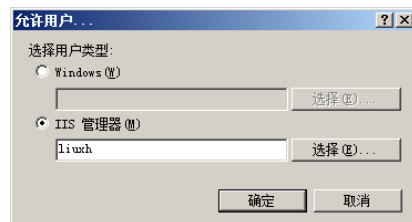


图 8-133 允许非 Windows 用户账户

③ 单击“确定”按钮，添加用户，如图 8-134 所示，可允许多个用户管理 IIS。如果需要删除某个用户，可选择相应的用户并单击“操作”窗格中的“拒绝用户”超级链接即可。

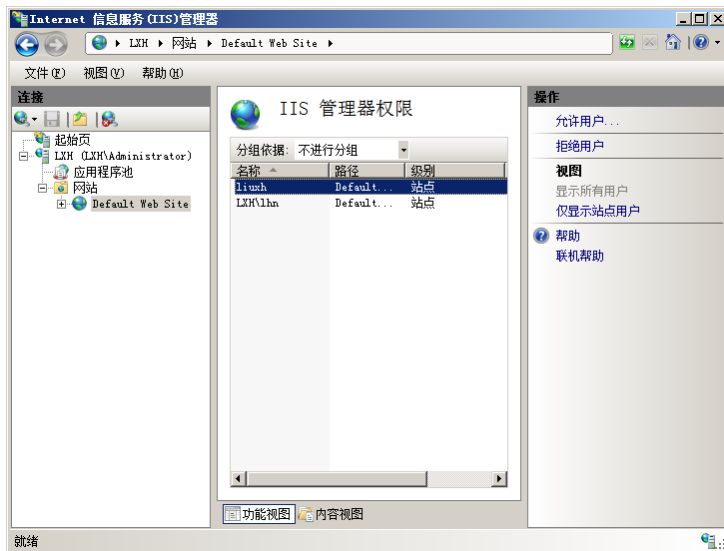


图 8-134 添加用户

8.8.5 远程管理 Web 站点

为 Web 服务器启用 IIS 远程管理功能以后，即可在安装了 IIS 7.0 的计算机中连接远程 Web 站点并进行管理。

① 在远程计算机中打开 IIS 管理器，默认显示“起始页”窗口，如图 8-135 所示。



图 8-135 “起始页”窗口

② 在“连接任务”列表框中单击“连接至站点”超级链接，显示如图 8-136 所示的“指定站点连接详细信息”对话框。在“服务器名称”文本框中键入待管理的 Web 站点所在的服务器名称或者 IP 地址，在“站点名称”文本框中键入 Web 站点的名称。

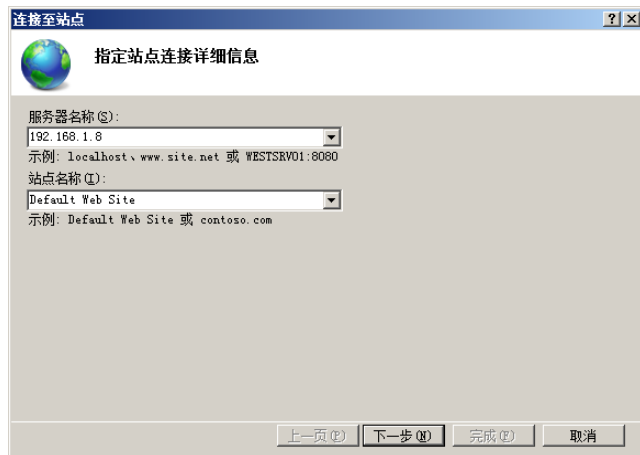


图 8-136 “指定站点连接详细信息”对话框

③ 单击“下一步”按钮，显示如图 8-137 所示的“提供凭据”对话框，在“用户名”文本框中键入管理用户名称。如果是 IIS 管理器用户，直接键入相应的用户名即可；如果是 Windows 用户，则应键入“服务器名称\用户名”，如 lxh\lhn。在“密码”文本框中键入相应密码。



图 8-137 “提供凭据”对话框

④ 单击“下一步”按钮，显示如图 8-138 所示的“服务器证书警报”对话框，提示证书已经发放到正在使用的服务器。

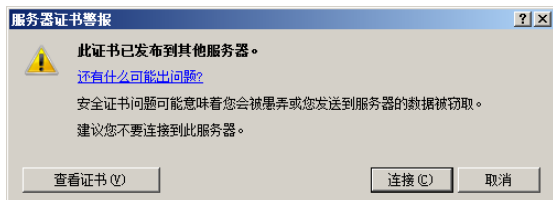


图 8-138 “服务器证书警报”对话框

⑤ 单击“查看证书”按钮，显示如图 8-139 所示的“证书”对话框，可以查看证书信息。单击“安装证书”按钮，安装此证书。

⑥ 单击“确定”按钮，返回“服务器证书警报”对话框。单击“连接”按钮，显示如图 8-140

所示的“指定连接名称”对话框，已经成功连接到授权管理的 IIS 站点。

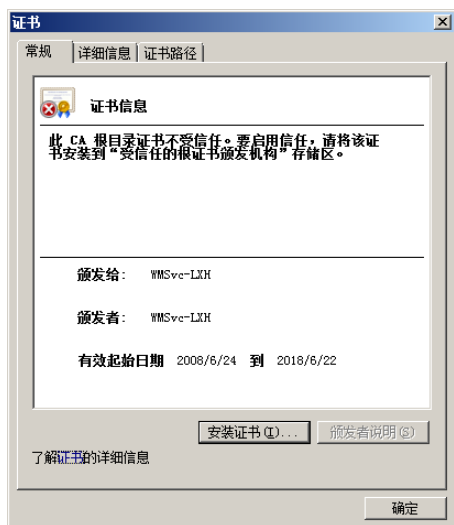


图 8-139 “证书”对话框

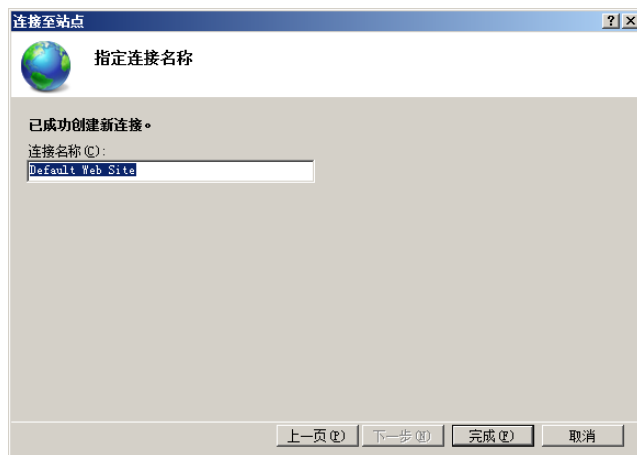


图 8-140 “指定连接名称”对话框

⑦ 单击“完成”按钮，连接到目标 Web 站点，如图 8-141 所示，在站点主页中可设置所需选项。



图 8-141 连接到远程 Web 站点

此时可管理远程服务器的 Web 站点，例如配置 Web 站点和 IIS 及管理虚拟目录等，如同在本地 Web 服务器上管理一样。

8.9 Windows Server 2003/2008 的配置差异

在 Windows Server 2003 中，IIS 的版本为 6.0，这是与 Windows Server 2008 最大的区别。在 Windows Server 2003 中，利用“配置您的服务器向导”安装 IIS（如图 8-142 所示），也可以在“添加或删除程序”中打开“Windows 组件向导”来安装。

安装完成 IIS 以后，单击“开始”→“管理工具”→“Internet 信息服务管理器”选项打开 IIS 管理器控制台，如图 8-143 所示。

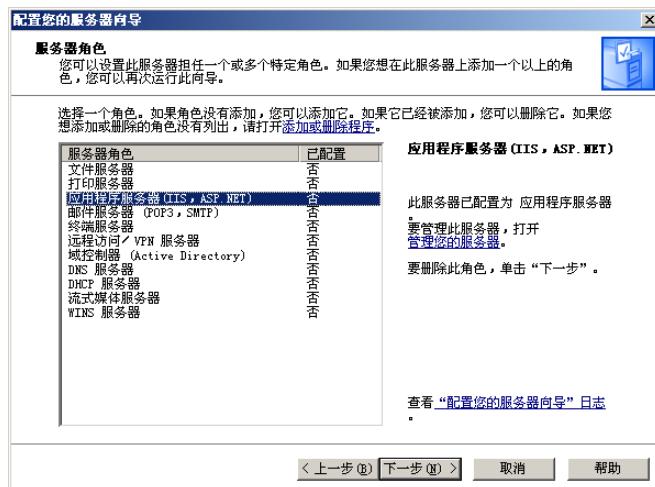


图 8-142 安装 IIS

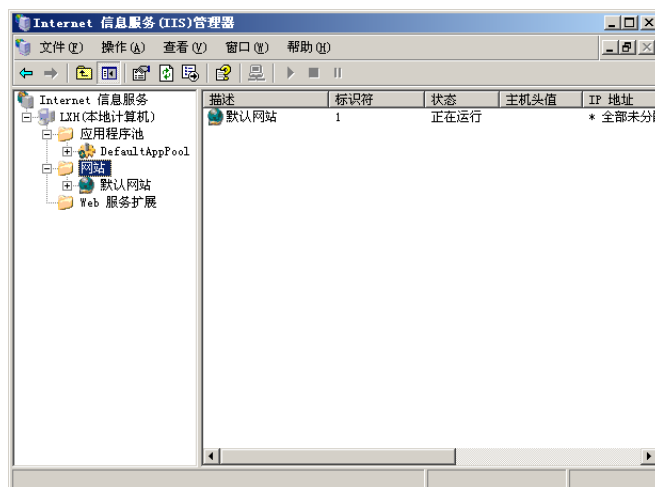


图 8-143 IIS 管理器控制台

所有的设置都可以在网站的属性对话框中完成（如图 8-144 所示），包括 IP 地址和端口、主目录、默认文档及身份验证等。

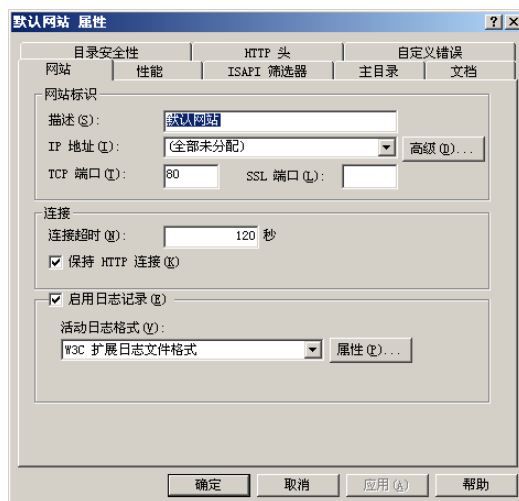


图 8-144 网站属性对话框

第 9 章 配置与管理 FTP 服务

虽然 Internet 上的文件传输工具层出不穷，但 FTP（File Transfer Protocol，文件传输协议）仍以其使用方便且安全可靠等特点长期占据着一席之地。FTP 是网络中最古老的文件传输服务，不仅可将文件从 FTP 服务器下载到客户端，也可将文件上传到 FTP 服务器。而且可以设置严格的文件权限，控制用户的访问。因此不仅可在不同计算机之间传输文件，还经常用来更新维护 Web 网站。

9.1 FTP 服务概述

FTP 不仅可在局域网中传输文件，而且可在 Internet 中使用。虽然 Web 服务也可以提供文件下载功能，但是 FTP 服务的效率更高。而且可以与 NTFS 相结合，设置更加严格的权限。

9.1.1 FTP 服务简介

FTP 服务和 Web 服务及文件服务一样，都可以提供文件传输功能。但是 Web 服务只能提供下载功能，无法上传文件；而文件服务虽然可以上传和下载，但只能应用于局域网，无法在 Internet 中使用。而 FTP 可以穿过路由，在 Internet/Intranet 中使用，这个特点通常用来更新维护 Web 网站。而且在 Windows 系统中，通常将 FTP 与 Web 服务一起安装。

另外，用户不仅可以在 FTP 服务器中设置权限，还可以和文件服务一样与 NTFS 权限结合使用，为文件设置 NTFS 权限，更加灵活地控制用户的访问。为文件设置了 NTFS 权限，即为 FTP 服务器指定了用户权限。用户在登录 FTP 站点时，必须使用 NTFS 权限中设置的用户账户及权限。

9.1.2 FTP 服务与 IIS

FTP 服务是 Windows Server 2003 和 Windows Server 2008 系统自带的功能，但 FTP 并不是一种独立的服务，而是集成于 IIS 中，可由用户选择安装。不过，Windows Server 2008 中的 IIS 7.0 没有集成 FTP 管理功能，用户安装以后仍需要使用 IIS 6.0 管理。

9.2 搭建与配置 FTP 服务器

FTP 服务器的安装与配置比较简单，在 Windows Server 2008 系统中安装 Web 服务器时可同时安装 FTP 服务器。安装完成以后需要指定 IP 地址、端口、主目录，以及欢迎和退出消息等。

9.2.1 安装 FTP 服务器

在 Windows Server 2008 中可利用“添加角色向导”来安装 FTP 服务器。

- ① 在“初始配置任务”或“服务器管理器”控制台中单击“添加角色”超级链接，运行“添加角色向导”。
- ② 在“选择服务器角色”对话框中选中“Web 服务器 (IIS)”复选框。
- ③ 单击“下一步”按钮，当显示“选择角色服务”对话框时选择“FTP 发布服务”复选框，显示如图 9-1 所示的“是否添加 FTP 发布服务所需的角色服务”对话框。

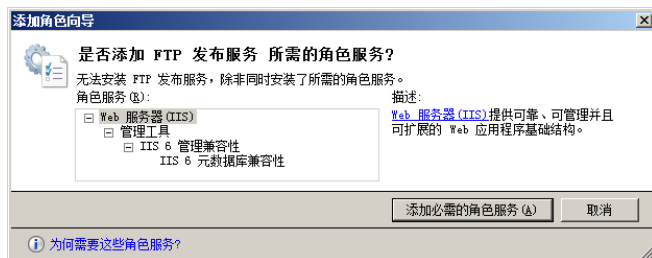


图 9-1 “是否添加 FTP 发布服务所需的角色服务”对话框

④ 单击“添加必需的角色服务”按钮，选中“FTP 发布服务”和“IIS 6 元数据库兼容性”复选框，如图 9-2 所示。如果仅安装 FTP 服务器，而不安装 Web 服务器，可清除“Web 服务器”复选框。

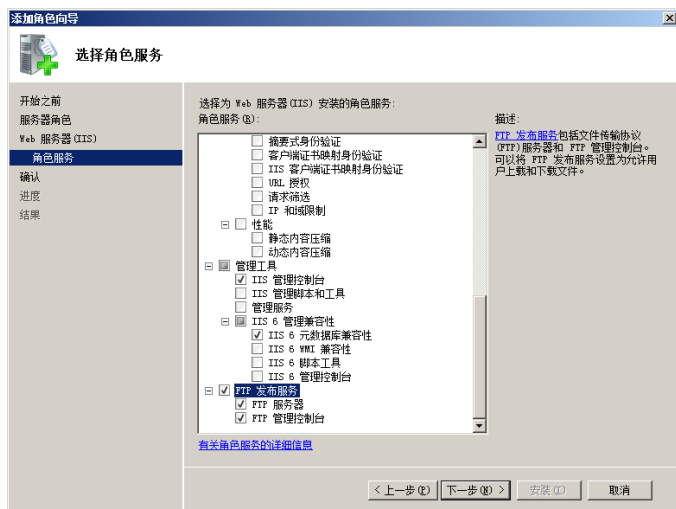


图 9-2 安装 FTP 服务

⑤ 单击“下一步”按钮，显示如图 9-3 所示的“确认安装选择”对话框，其中列出待安装的服务。



图 9-3 “确认安装选择”对话框

⑥ 单击“安装”按钮，开始安装 FTP 服务器。完成后显示如图 9-4 所示的“安装结果”对话框，提示安装成功。



图 9-4 “安装结果”对话框

⑦ 单击“关闭”按钮关闭，单击“开始”→“管理工具”→“Internet 信息服务 (IIS) 6.0 管理器”选项，显示“Internet 信息服务 (IIS) 6.0 管理器”窗口。默认状态下，已经创建了一个 FTP 站点，并且为“停止”状态，如图 9-5 所示。

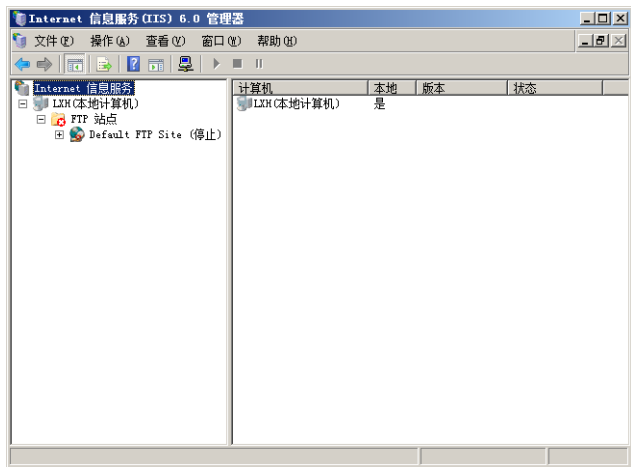


图 9-5 创建的 FTP 站点

⑧ 右击已停止的 FTP 站点，选择快捷菜单中的“启动”选项启动该站点，如图 9-6 所示。

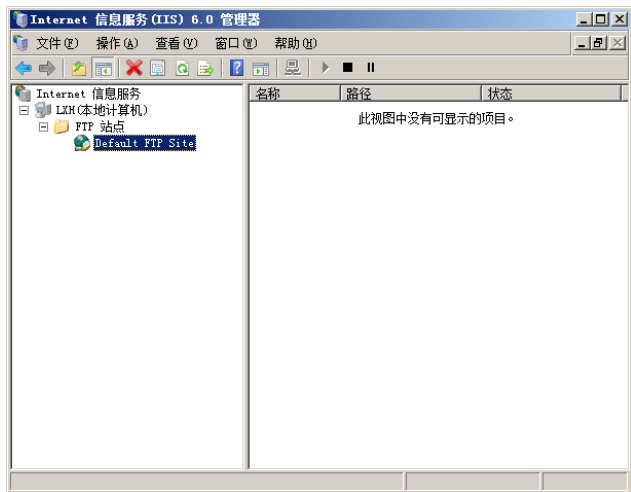


图 9-6 启动 FTP 站点

9.2.2 设置 IP 地址和端口号

新安装的 FTP 服务器的默认 IP 地址为“全部未分配”方式，即 FTP 网站与服务器中所有的 IP 地址绑定在一起，默认 TCP 端口为 21。这种状态下，FTP 客户端可以使用该服务器中的任何 IP 地址及默认端口访问。因此为了安全起见，应为 FTP 网站指定唯一的 IP 地址和端口。

① 在 IIS 6.0 管理器窗口中选择 FTP 站点，右击并选择快捷菜单中的“属性”选项，显示如图 9-7 所示的 FTP 站点属性对话框。

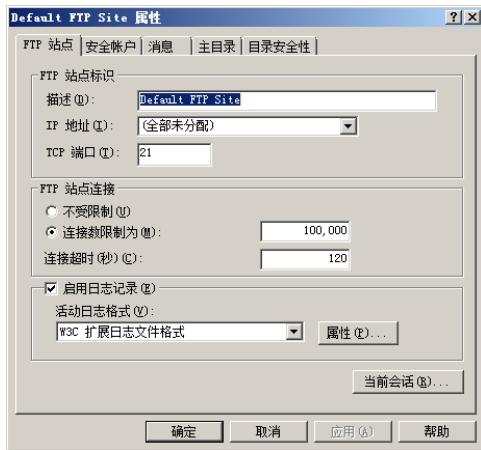


图 9-7 FTP 站点属性对话框

在“FTP 站点标识”选项组中设置如下选项。

描述：设置该 FTP 站点的标识，仅用于与其他 FTP 站点区分。

IP 地址：如果 FTP 服务器绑定有多个 IP 地址，则应在“IP 地址”下拉列表框中指定唯一的 IP 地址，使客户端只能通过这一个 IP 地址访问该 FTP 服务器。尤其在创建多个 FTP 站点后，应为每个 FTP 站点都指定一个唯一的 IP 地址。

TCP 端口：FTP 服务的默认 TCP 端口为“21”。如果服务器只有一个 IP 地址，却要实现多个不同 FTP 站点，就可以通过修改端口来实现一个 IP 多站点的共存。

② 单击“确定”按钮保存设置。

如果 FTP 服务器使用默认端口 21，那么客户端访问时不必输入端口号，系统会自动使用默认的 21 端口。例如，ftp://192.168.1.16。如果更改了默认的 TCP 端口号，则客户端访问时必须输入相应的端口号。例如，ftp://192.168.1.16:33。如果客户端不知道正确的端口号，则无法访问。

9.2.3 限制连接数量

FTP 服务器用来提供文件的上传和下载，如果同时从 FTP 服务器传输文件的用户数量比较多，就会占用大量带宽，影响其他网络服务的正常运行。如果服务器的配置较低且性能较差，还会造成系统响应迟缓甚至瘫痪。尤其在一些中小型企业中，往往一台服务器兼做多种网络服务，如 Web 及 E-mail 等。当并发访问数量较多时，更会因带宽被大量占用造成服务中断或超时，因此应对 FTP 连接数量进行一定的限制。

打开 FTP 站点属性对话框，在“FTP 站点”选项卡的“FTP 站点连接”选项组中可以设置如下选项。

(1) 不受限制：不限制连接数量。如果服务器配置和网络带宽都较高，或者仅为网络内部提供访问服务时，可选择该单选按钮。

(2) 连接数限制为：设置限制同时连接到该站点的连接数量，即允许同时连接该 FTP 站点的最大用户数量。

(3) 连接超时：设置多长时间内（以秒为单位）如果用户没有活动，则断开服务器连接。以及时释放系统性能和网络带宽，减少系统资源和网络资源浪费，默认为 120 秒。

9.2.4 设置主目录

FTP 服务器的主目录即 FTP 站点的根目录，其中保存 FTP 站点中所有文件的文件夹，通常位于本地磁盘或网络磁盘中。当 FTP 客户端访问该 FTP 站点时，即访问主目录文件夹。

① 打开 FTP 站点属性对话框，打开“主目录”选项卡，如图 9-8 所示。如果要将 FTP 主目录指定为本地计算机中的某个文件夹、磁盘或卷，则选择“此计算机上的目录”单选按钮。并在“本地路径”文本框中键入路径即可，也可单击“浏览”按钮选择。

如果要将 FTP 主目录指定为网络中某台计算机中的共享文件夹，则选择“另一计算机上的目录”单选按钮。然后在“网络共享”文本框中键入网络共享文件夹的路径，格式为“\\计算机名或 IP 地址\共享名”。例如，\\192.168.1.100\coolpen，如图 9-9 所示。

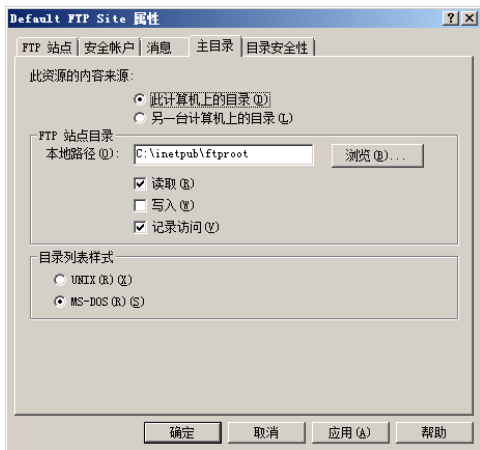


图 9-8 “主目录”选项卡

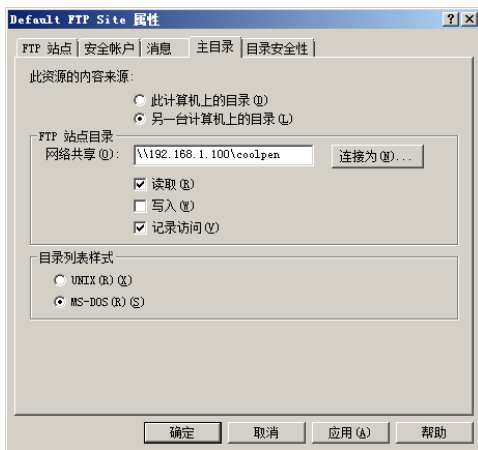


图 9-9 设置 FTP 主目录



使用该方式时，待指定的网络计算机必须已经连入网络并已将待使用的文件夹设置为共享。



② 设置主目录以后，设置如下目录访问权限。

读取：允许用户查看或下载 FTP 主目录中的文件，但不允许上传或更改文件。

写入：不仅允许用户下载 FTP 主目录中的文件，还允许向主目录中上传文件。通常只向特权用户开放，以保证 FTP 服务器的安全。

记录访问：启用日志功能，将访问目录的活动记录在日志文件中。默认情况下，日志被启用。

③ 单击“确定”按钮保存设置。

9.2.5 设置欢迎和退出消息

为了使得 FTP 网站更加人性化，同时也为企业网站起到宣传的作用，通常会为 FTP 网站设置欢迎消息。当用户登录到 FTP 网站时，显示欢迎及说明信息；当用户退出 FTP 网站时，显示欢送消息。

(1) 打开 FTP 站点的属性对话框，打开“消息”选项卡，显示如图 9-10 所示。

在其中设置“横幅”、“欢迎”、“退出”和“最大连接数”选项。

横幅：用户连接到 FTP 服务器时所显示的消息，通常为 FTP 站点的名称。

欢迎：当用户连接到 FTP 服务器后显示的消息，通常包括向用户致意、使用该 FTP 站点时应注意

的问题、管理者的联络方式，以及上载或下载的规则说明等。

退出：当用户从 FTP 服务器注销时显示的消息，通常为欢迎用户再次光临及向用户表示感谢等内容。

最大连接数：用户试图连接到 FTP 服务器，但该 FTP 服务已达到允许的最大客户端连接数而导致失败时，将显示此消息。

(2) 单击“确定”按钮保存设置。

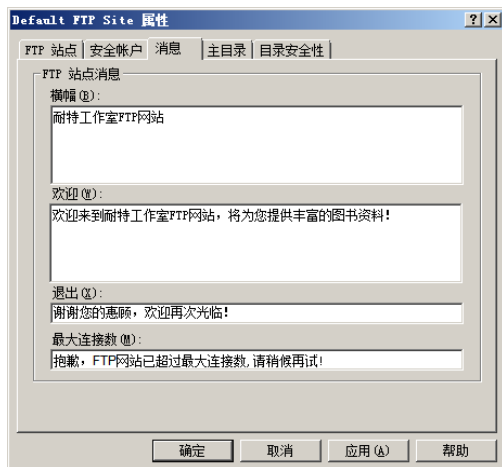


图 9-10 “消息”选项卡

9.2.6 设置访问安全

FTP 站点中往往存储着重要的数据，甚至可能是 Web 网站的主目录，对安全性要求较高。但是默认状态下，允许来自任何 IP 地址的计算机访问。因此为安全起见，应防止被随意访问，或者限制特定的 IP 地址访问。通常可以通过禁止匿名访问，或者限制 IP 地址访问，从而确保 FTP 站点的安全。

1. 禁止匿名访问

默认状态下，FTP 站点允许用户匿名连接，即用户无须输入用户名和密码即可访问 FTP 服务器中的文件。不过，如果 FTP 站点中存储有重要或敏感的信息，只允许授权用户访问，那么应当禁用匿名访问。

打开 FTP 站点的属性对话框，打开“安全账户”选项卡，如图 9-11 所示。默认选中“允许匿名连接”复选框，允许用户匿名访问该 FTP 站点。

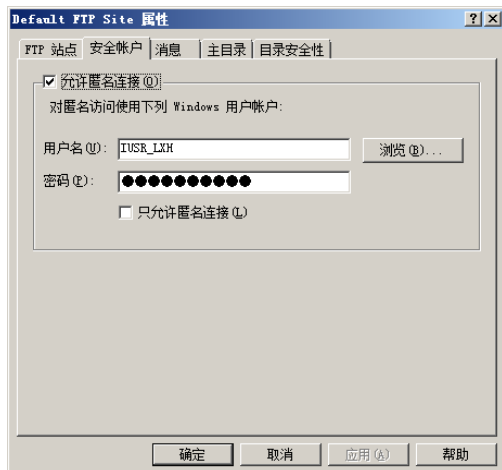


图 9-11 “安全账户”选项卡

如果要禁止用户匿名访问该 FTP 站点，单击“允许匿名连接”复选框，显示如图 9-12 所示的警告框。单击“是”按钮，清除该复选框。

当禁止匿名用户连接后，只有 FTP 服务器或活动目录中有效的用户账户才能通过身份认证，访问该 FTP 站点。

2. 限制 IP 地址访问

为了保证 FTP 服务器的安全，可以限制用户的 IP 地址。即只允许信任的 IP 地址访问，而拒绝不受信任的 IP 地址访问。避免来自外界的恶意攻击，提高 FTP 站点访问的安全性。特别是对于企业内部 FTP 站点而言，采用 IP 地址限制的方式非常简单并有效。

在 FTP 站点的属性对话框中，打开“目录安全性”选项卡，如图 9-13 所示，在其中设置要限制的 IP 地址。

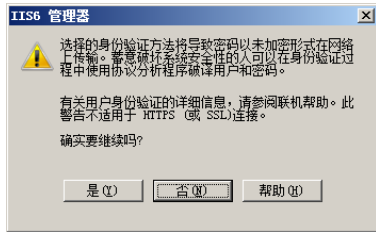


图 9-12 警告框



图 9-13 “目录安全性”选项卡

如果设置为“授权访问”，那么所有计算机都具备访问 FTP 服务器的权限，而添加到列表中的计算机将不允许访问 FTP 站点。

① 在“目录安全性”选项卡中选择“授权访问”单选按钮，单击“添加”按钮，显示如图 9-14 所示的“拒绝访问”对话框。如果要限制单台计算机对 FTP 站点的访问，可选择“一台计算机”单选按钮，并在“IP 地址”文本框中键入拒绝访问的 IP 地址即可。

如果要限制一个 IP 地址段的计算机，则选择“一组计算机”单选按钮。在“网络标识”文本框中键入标识的 IP 地址，在“子网掩码”文本框中键入该网段的子网掩码，如图 9-15 所示。

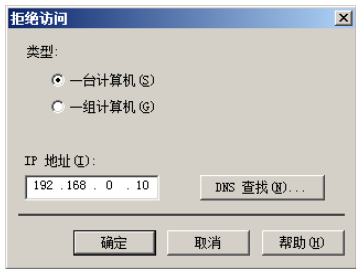


图 9-14 “拒绝访问”对话框

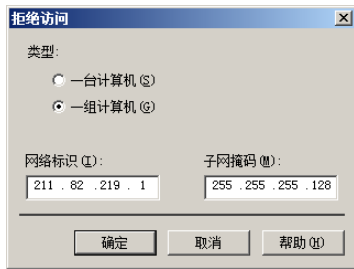


图 9-15 限制一组 IP 地址

② 单击“确定”按钮，将该 IP 地址或 IP 地址段添加到“下列除外”列表框中。访问方式为“拒绝”，如图 9-16 所示。重复上述操作步骤，可添加多个 IP 地址或 IP 地址段。

如果设置为“拒绝访问”，那么所有计算机都不允许访问 FTP 站点，而只有添加到列表中的计算机才允许访问。

① 在“目录安全性”选项卡中选择“拒绝访问”单选按钮，单击“添加”按钮，显示如图 9-17

所示的“授权访问”对话框。如果要添加允许访问 FTP 站点的单台计算机，可选择“一台计算机”单选按钮，并在“IP 地址”文本框中键入要授权访问的 IP 地址。



图 9-16 拒绝访问的 IP 地址

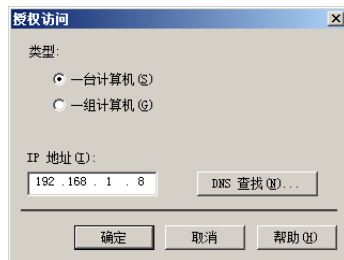


图 9-17 “授权访问”对话框

如果要添加允许访问的一组计算机，选择“一组计算机”单选按钮，如图 9-18 所示。在“网络标识”文本框中键入标识的 IP 地址，在“子网掩码”文本框中键入该网段的子网掩码。

② 单击“确定”按钮，将该 IP 地址或 IP 地址段添加到“下列除外”列表框中。访问方式为“允许”，如图 9-19 所示。重复上述操作步骤，可添加多个 IP 地址或 IP 地址段。

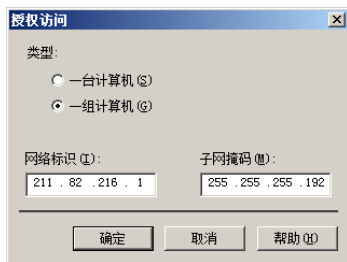


图 9-18 允许一组 IP 地址



图 9-19 允许访问的 IP 地址

9.2.7 设置用户访问权限

在设置 FTP 站点时，只能简单地设置“读取”和“写入”权限，并且默认本地服务器或域中所有的用户都具有访问权限。因此通常将 FTP 服务器与 NTFS 权限相结合，和文件服务器一样为 FTP 站点中的文件设置更加详细的权限，以满足不同用户的使用。

1. 设置 NTFS 权限

在 Windows 资源管理器中选择 FTP 站点主目录或虚拟目录文件夹，右击并选择快捷菜单中的“属性”选项，打开文件夹属性对话框。打开“安全”选项卡，如图 9-20 所示。在“组或用户名”文本框中显示可以访问 FTP 文件夹的用户账户，选择一个用户，在权限列表框中显示该用户所拥有的访问权限。

为了严格控制用户的权限，可删除其他用户，然后添加允许访问 FTP 文件夹的用户。不过默认状态下，用户的权限是从其父文件夹继承来的。因此无法删除现在用户，需要取消继承关系，然后设置

用户权限。这里以设置用户账户 lhn 访问 coolpen 文件夹的访问权限为例介绍。

为取消继承关系，执行如下操作。

① 在“安全”选项卡中单击“高级”按钮，显示如图 9-21 所示的“coolpen 的高级安全设置”对话框，其中显示不同账户所拥有的权限。

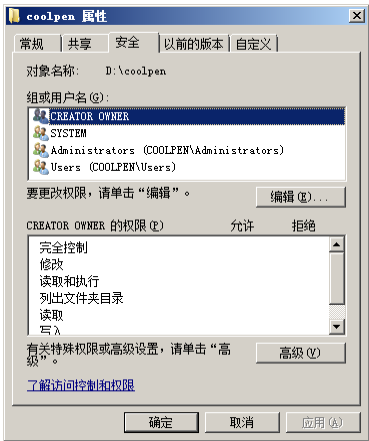


图 9-20 “安全”选项卡



图 9-21 “coolpen 的高级安全设置”对话框

② 单击“编辑”按钮，显示如图 9-22 所示的对话框，用来更改高级安全设置。

③ 单击“包括可从该对象的父项继承的权限”复选框，显示如图 9-23 所示的“Windows 安全”对话框。



图 9-22 更改高级安全设置

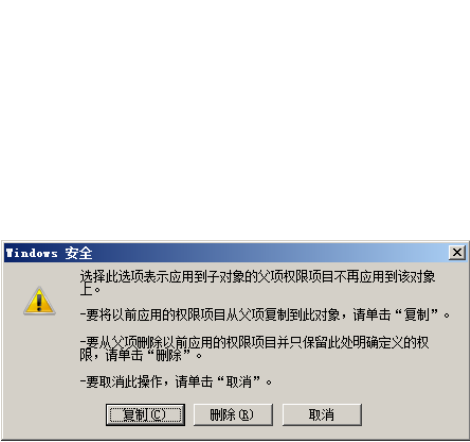


图 9-23 “Windows 安全”对话框

④ 单击“删除”按钮，删除权限继承，并清除“包括可从该对象的父项继承的权限”复选框，依次单击“确定”按钮返回“安全”选项卡。可以看到只保留了 Administrators 用户组，其他所有账户已被删除，如图 9-24 所示。

此时即可添加用户并设置 NTFS 权限。

设置用户权限的操作步骤如下。

① 在文件夹属性对话框的“安全”选项卡中单击“编辑”按钮，显示如图 9-25 所示的“coolpen 的权限”对话框，默认只保留 Administrators 用户组。

② 单击“添加”按钮，显示如图 9-26 所示的“选择用户、计算机或组”对话框。在“输入对象名称来选择”文本框中键入待分配读写权限的用户，例如 lhn，或者单击“高级”按钮查找。

③ 单击“添加”按钮，添加该用户并返回“coolpen 的权限”对话框。选择新添加的用户，在权限列表框中为其选择待分配的权限。共有 6 种权限，即完全控制、修改、读取和执行、列出文件夹目

录、读取和写入。单击“确定”按钮保存并返回“安全”选项卡。

④ 如果要为该用户分配更详细的权限，则在“安全”选项卡中单击“高级”按钮。显示“coolpen 的高级安全设置”对话框，单击“编辑”按钮，显示如图 9-27 所示的对话框。

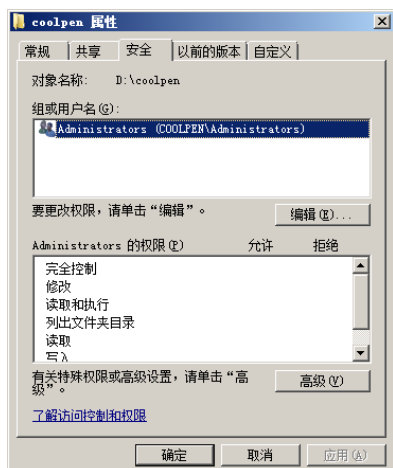


图 9-24 取消权限继承

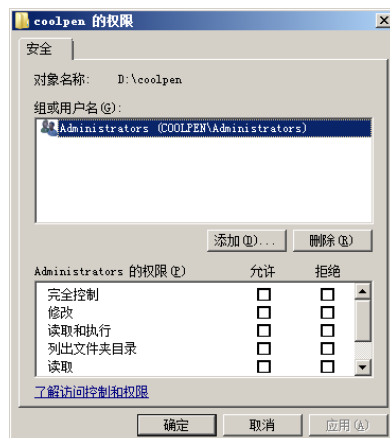


图 9-25 “coolpen 的权限”对话框

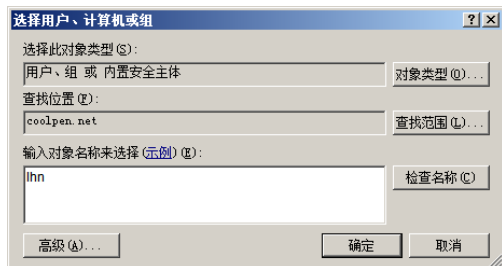


图 9-26 “选择用户、计算机或组”对话框

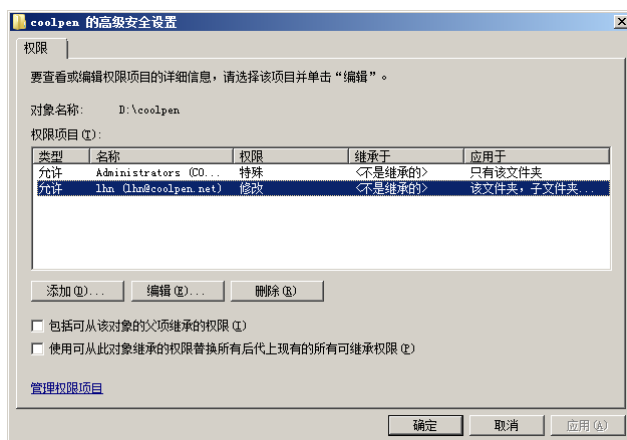


图 9-27 更改高级安全设置

⑤ 在“权限项目”列表框中选择待设置的用户账户，单击“编辑”按钮，显示如图 9-28 所示的“coolpen 的权限项目”对话框，在“权限”列表框中选择更详细的权限，共有 14 种权限可供选择。

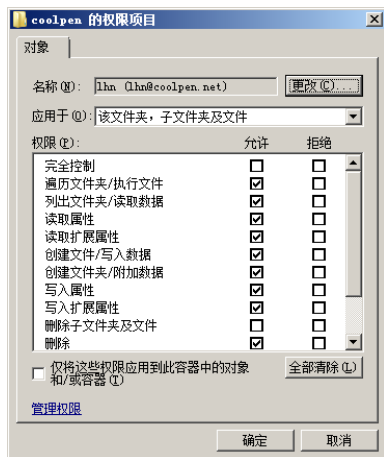


图 9-28 “coolpen 的权限项目”对话框

⑥ 依次单击“确定”按钮保存设置。

利用这种方式设置的用户权限更加详细，可以精确到是否允许用户读取、删除、删除子文件夹和文件，以及创建文件或文件夹等，从而可以更好地控制用户对 FTP 文件夹的访问。

2. 设置磁盘配额

默认情况下，FTP 服务器并未限制用户上传文件的总大小。因此当为 FTP 用户赋予了写入权限时，用户就可以向 FTP 服务器中上传任意大小的文件，从而导致服务器中宝贵的硬盘空间被迅速占用。为了保护硬盘空间，应当启用磁盘配额功能来限制每个用户使用磁盘空间的大小。

不过，FTP 服务器本身并没有提供磁盘限额功能，需要借助 Windows Server 2008 系统中 NTFS 文件系统来实现。因此 FTP 主目录必须位于 NTFS 格式的分区，FAT32 文件系统无法设置磁盘配额。

为用户设置了磁盘配额以后，当用户上传的文件超出空间限制或者到警告等级时，系统将自动发出警告，提示用户超出空间配额，上传操作不能完成等信息。关于磁盘配额的设置，请参见本书中的相关内容，这里不再赘述。

9.2.8 启动与停止 FTP 服务器

如果要停止 FTP 服务的运行，可选择待停止的 FTP 站点，右击并选择快捷菜单中的“停止”选项即可，选择“启动”选项则可启动 FTP 站点。

9.3 创建与管理虚拟站点

FTP 服务和 Web 服务一样，也具有虚拟网站功能。可以在一台服务器上搭建多个 FTP 站点，为用户提供不同的 FTP 服务。而且不同 FTP 站点可以单独配置和管理，拥有不同的 IP 地址和端口号。并且设置不同的用户权限，从而扩大服务器的功能。

9.3.1 虚拟站点概述

要在一台服务器上创建多个 FTP 站点为不同需求的用户提供不同的文件服务，例如，为多个 Web 站点的内容进行更新时，就可以利用虚拟站点来实现。

多个虚拟 FTP 站点可以位于同一台或多台服务器，而且每个 FTP 站点都相当于一台独立的 FTP 服务器。可以分别设置不同的访问权限，为用户提供不同的上传和下载服务。每个虚拟 FTP 站点都拥有自己的 IP 地址和主目录，可以单独配置和管理，独立启动、暂停和停止。并且均能够建立虚拟目录，与默认 FTP 站点几乎没有任何区别。

利用虚拟 FTP 站点可以有效地分离敏感信息，从而提高数据的安全性，并便于数据的管理。

9.3.2 虚拟站点的创建方式

在同一台服务器上创建多个 FTP 虚拟站点通常有两种方式，即利用 IP 地址和端口来实现。用户访问如同分别访问不同服务器一样，这两种方式的区别如下。

(1) 利用不同的 IP 地址创建：如果服务器绑定有多个 IP 地址，就可以利用这种方式创建，为每个 FTP 站点各指定一个唯一的 IP 地址。

(2) 利用不同的端口创建：如果服务器只有一个 IP 地址，就可以得用不同的端口创建不同的 FTP 站点。不过，用户访问时也必须加上端口才能访问，例如，ftp://192.168.1.9:33。

9.3.3 使用 IP 地址创建

使用 IP 地址创建虚拟站点的操作步骤如下。

① 在 IIS 6.0 管理器中右击“FTP 站点”，选择快捷菜单中的“新建”→“FTP 站点”选项，显示如图 9-29 所示的“FTP 站点创建向导”对话框。

② 单击“下一步”按钮，显示如图 9-30 所示的“FTP 站点描述”对话框。在“描述”文本框中键入 FTP 站点的描述，以便于和其他站点相区分。

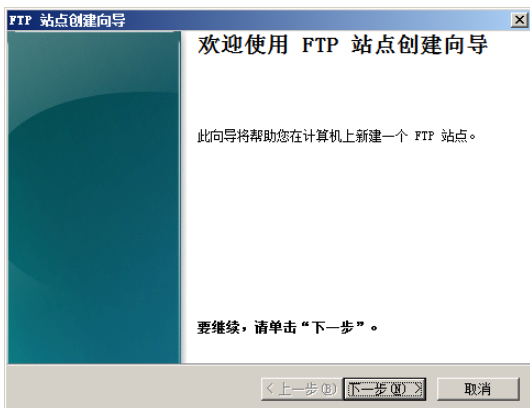


图 9-29 “FTP 站点创建向导”对话框

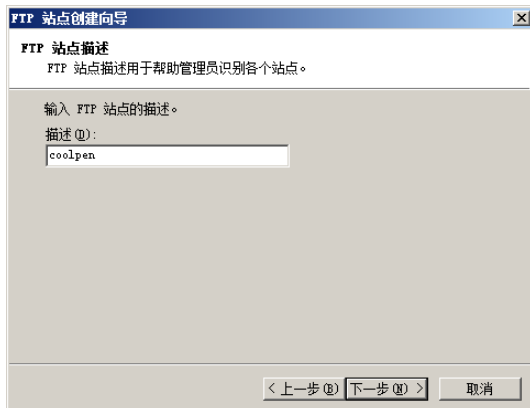


图 9-30 “FTP 站点描述”对话框

③ 单击“下一步”按钮，显示如图 9-31 所示的“IP 地址和端口设置”对话框。在“输入此 FTP 站点使用的 IP 地址”下拉列表框中为该 FTP 站点选择唯一的 IP 地址，在“输入此 FTP 站点的 TCP 端口”文本框中键入 FTP 站点使用的端口，使用默认的 21 端口即可。

④ 单击“下一步”按钮，显示如图 9-32 所示的“FTP 用户隔离”对话框。

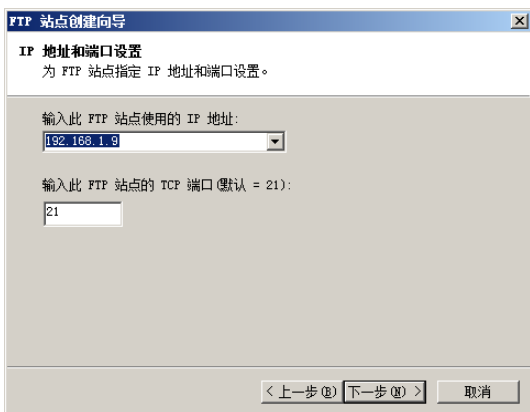


图 9-31 “IP 地址和端口设置”对话框

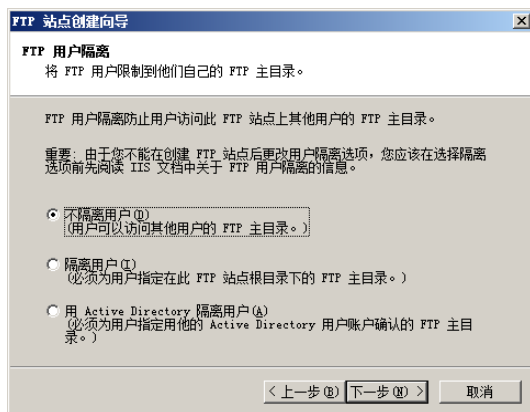


图 9-32 “FTP 用户隔离”对话框

在其中设置如下选项。

不隔离用户：不启用 FTP 用户隔离，用户可以访问整个 FTP 站点。适合于只提供文件下载功能，或者不需要在用户间进行数据访问保护的 FTP 站点。

隔离用户：每个用户登录 FTP 时都需要验证，并限制在自己的主目录中，不允许浏览用户主目录外的内容。适合用于为 Web 网站提供维护服务，或者提供文件备份和存储服务的服务器。不过如果创建的站点过多，将会影响服务器性能。

用 Active Directory 隔离用户：只能在域环境中应用，用户的主目录可放置在网络中的任意服务器中。该模式需要 Active Directory 服务器和文件服务器的支持，并且为所有允许连接 FTP 服务的用户（包括匿名账户）创建共享和用户目录，以便用户建立到 FTP 服务器的本地路径。该模式只在局域网中使用。

⑤ 单击“下一步”按钮，显示如图 9-33 所示的“FTP 站点主目录”对话框。在“路径”文本框中键入 FTP 站点的主目录路径，或者单击“浏览”按钮选择。

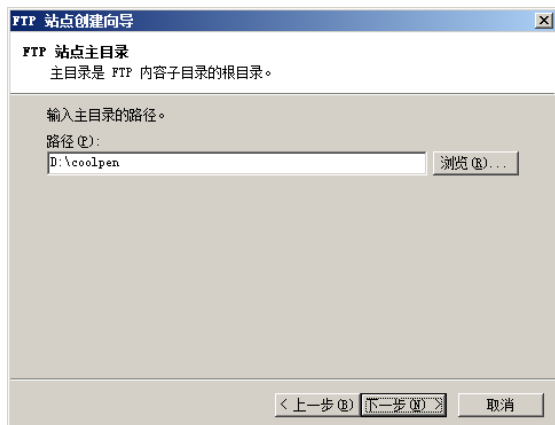


图 9-33 “FTP 站点主目录”对话框

⑥ 如果要将网络中的共享文件夹作为 FTP 站点主目录，则路径格式为“\\计算机名或 IP 地址\共享文件夹名”。单击“下一步”按钮，显示如图 9-34 所示的“FTP 站点安全凭据”对话框，在“用户名”和“密码”文本框中分别键入访问共享文件夹的用户名和密码。

⑦ 单击“下一步”按钮，显示如图 9-35 所示的“FTP 站点访问权限”对话框，在其中选择用户访问该 FTP 站点的读写权限。

⑧ 单击“下一步”按钮，显示如图 9-36 所示的“已成功完成 FTP 站点创建向导”对话框。

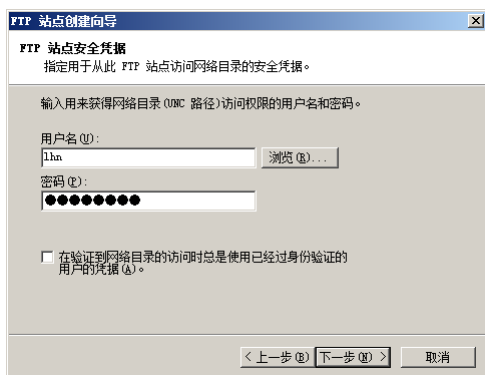


图 9-34 “FTP 站点安全凭据”对话框

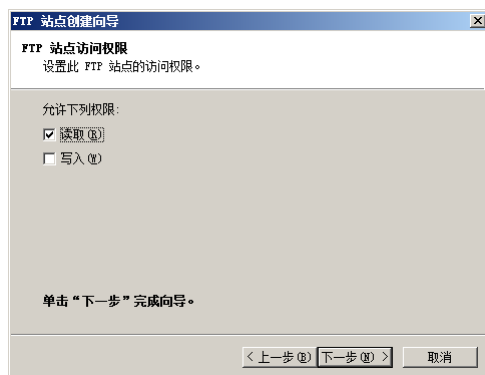


图 9-35 “FTP 站点访问权限”对话框

⑨ 单击“完成”按钮，创建完成 FTP 站点，如图 9-37 所示。

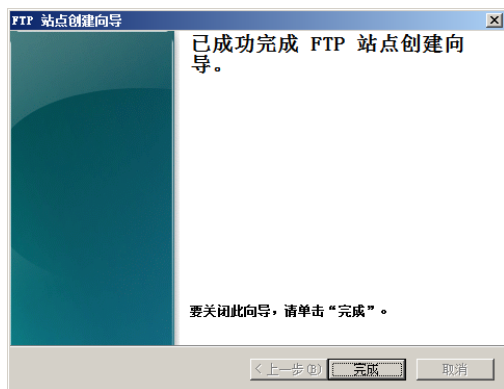


图 9-36 “已成功完成 FTP 站点创建向导”对话框

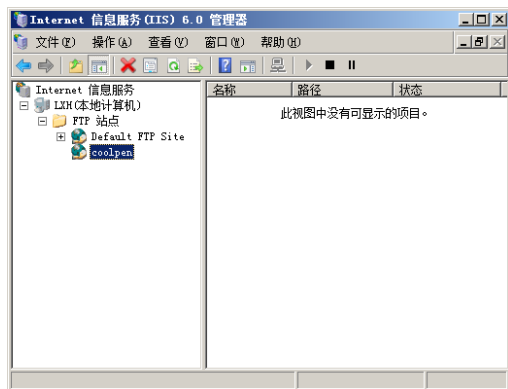


图 9-37 创建完成 FTP 站点

9.3.4 使用端口号创建

使用端口号创建虚拟 FTP 站点的过程和使用 IP 地址创建的过程类似，同样可利用“FTP 站点创

建向导”来完成。不同的是在“IP 地址和端口设置”对话框中的“输入此 FTP 站点的 TCP 端口”文本框中设置端口号，如图 9-38 所示。



图 9-38 设置 FTP 端口号

9.3.5 管理虚拟站点

虚拟站点的管理方式和默认 FTP 站点完全相同，均可在其属性对话框中管理（如图 9-39 所示），如指定 IP 地址和端口及设置访问权限等。具体操作可参见前面所述内容，这里不再赘述。

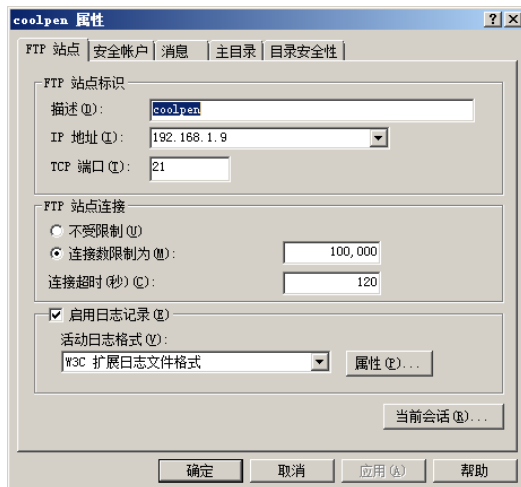


图 9-39 管理虚拟站点

9.4 创建与管理虚拟目录

如果要扩展虚拟网站，为不同上传或下载服务的用户提供不同的目录，就可以利用虚拟目录来实现。使用虚拟目录可以创建多个不同内容且不同访问权限的目录，并且可以位于不同磁盘或计算机中，而用户访问时如同位于同一个 FTP 网站一样。

9.4.1 虚拟目录概述

FTP 虚拟目录是 FTP 网站的下一级目录，和 Web 服务器的虚拟目录一样，也指定为某一个文件夹，并且可以位于其他磁盘或网络中的其他服务器。但用户访问不同虚拟目录中的文件时，如同位于同一个 FTP 网站一样。

虚拟目录具有以下意义。

- (1) 便于扩展：当 FTP 网站升级或扩充时需要扩展磁盘空间，此时只需创建新的虚拟目录并指定

为新的磁盘或卷即可，不会影响用户的访问。

(2) 增删灵活：可以根据需要随时向 FTP 网站中添加或者删除虚拟目录，而且在添加或移除虚拟目录时不会影响 FTP 网站的运行。

(3) 易于配置：虚拟目录与虚拟网站使用相同的 IP 地址和端口号，不会产生冲突。同时新建的虚拟目录将自动继承 FTP 网站的权限，管理更加简单。

虚拟目录不是一个独立 FTP 站点，它要依附于某个 FTP 网站之下。即没有独立的 DNS 域名、IP 地址或端口号，用户必须通过访问虚拟网站才能访问虚拟目录。

9.4.2 虚拟目录的创建方式

IIS 提供了虚拟目录创建向导，可以帮助管理员轻松完成虚拟目录的创建和发布。

① 在 IIS 6.0 管理器中展开“FTP 站点”，选择待创建虚拟目录的 FTP 站点。右击并依次选择快捷菜单中的“新建”→“虚拟目录”选项，显示“虚拟目录创建向导”对话框，如图 9-40 所示。

② 单击“下一步”按钮，显示如图 9-41 所示的“虚拟目录别名”对话框。在“别名”文本框中键入虚拟目录的别名，该别名是用户访问虚拟目录时的名称，同时也用于与其他虚拟目录相区分。

③ 单击“下一步”按钮，显示如图 9-42 所示的“FTP 站点内容目录”对话框。在“路径”文本框中键入该虚拟目录要使用的文件夹路径，或者单击“浏览”按钮选择。该路径既可以位于本地磁盘，也可以是网络中计算机的共享文件夹。如果是共享文件夹，则格式为“\\计算机名或 IP 地址\共享名”。

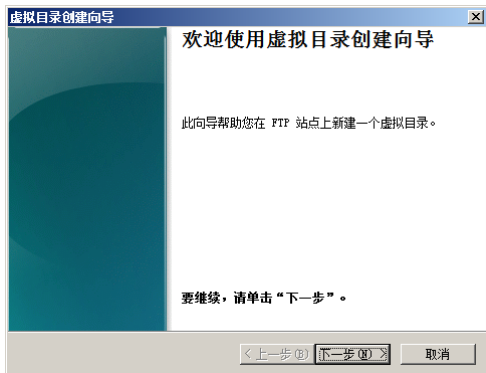


图 9-40 “虚拟目录创建向导”对话框

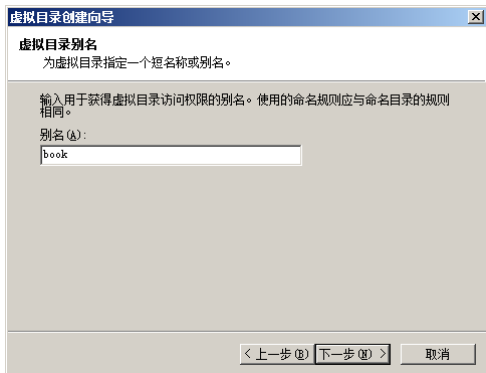


图 9-41 “虚拟目录别名”对话框

④ 单击“下一步”按钮，显示如图 9-43 所示的“虚拟目录访问权限”对话框。选择该虚拟目录的用户访问权限，可以选择“读取”或“写入”权限。

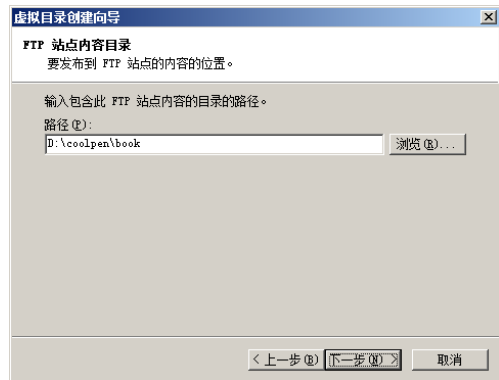


图 9-42 “FTP 站点内容目录”对话框

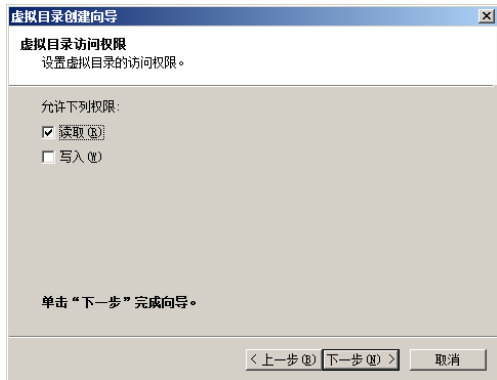


图 9-43 “虚拟目录访问权限”对话框

⑤ 单击“下一步”按钮，显示如图 9-44 所示的“已成功完成虚拟目录创建向导”对话框。

⑥ 单击“完成”按钮，创建完成虚拟目录并显示在 IIS 管理器中，如图 9-45 所示。

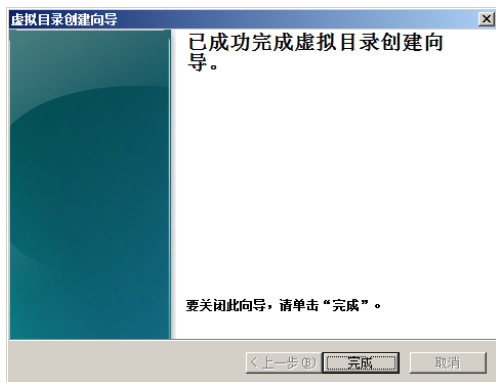


图 9-44 “已成功完成虚拟目录创建向导”对话框

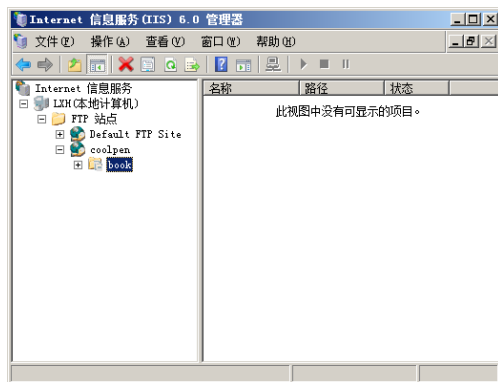


图 9-45 创建完成的虚拟目录

9.4.3 管理虚拟目录

创建完成虚拟目录以后，即可像虚拟网站一样管理。不过虚拟目录的属性对话框中只有“虚拟目录”和“目录安全性”选项卡，可配置的选项较少。不能设置 IP 地址、端口、连接数量和欢迎消息，只能配置主目录、访问权限及 IP 地址访问控制。

在 IIS 6.0 管理器中展开 FTP 网站，选择待管理的虚拟目录。右击并选择快捷菜单中的“属性”选项，显示如图 9-46 所示的虚拟目录属性对话框，在其中可设置虚拟目录。

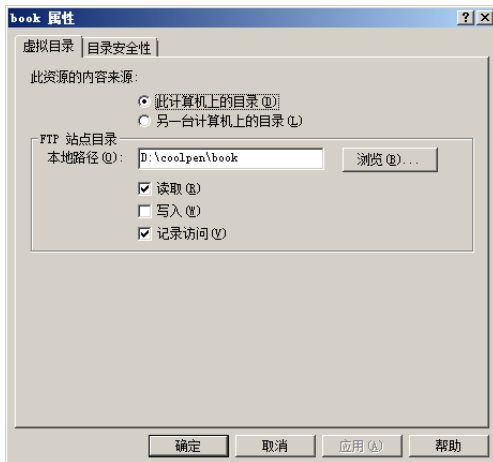


图 9-46 “虚拟目录属性”对话框

9.5 使用 Serv-U 搭建 FTP 服务器

Serv-U 是当前最流行的 FTP 服务器搭建软件之一，可运行在所有版本的 Windows 操作系统中，可以很方便地为不同的用户设置不同的访问权限。Serv-U 安装简单、易于配置且功能强大，是中小企业网络用户理想的 FTP 服务器软件。

9.5.1 搭建 Serv-U 服务器

Serv-U 可以为每个用户设置访问权限和磁盘配额，即使是在 FAT32 分区中也如此，其最新版本可以到官方网站（<http://www.serv-u.com>）或者国内的一些下载站点下载。

1. 安装 Serv-U

① 运行 Serv-U 安装程序，显示如图 9-47 所示的“选择安装语言”对话框，在下拉列表框中选择“简体中文”选项。

- ② 单击“确定”按钮，显示如图9-48所示的Serv-U安装向导。

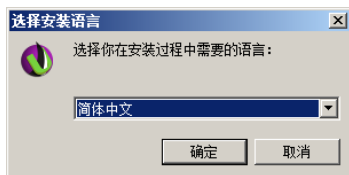


图 9-47 “选择安装语言”对话框



图 9-48 Serv-U 安装向导

- ③ 单击“下一步”按钮，显示如图9-49所示的“许可证”对话框。选择“我同意”单选按钮，接受许可协议。

- ④ 单击“下一步”按钮，显示如图9-50所示的“选择安装文件夹”对话框。单击“浏览”按钮可选择安装路径，也可使用默认安装路径。

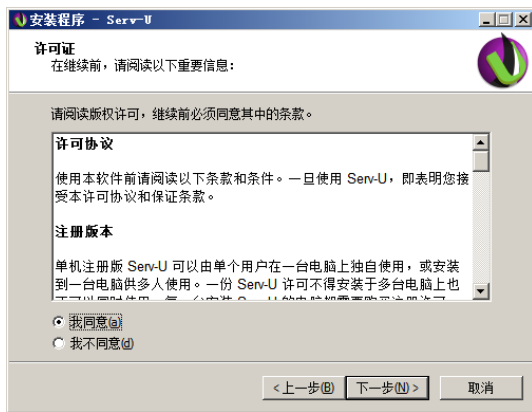


图 9-49 “许可证”对话框



图 9-50 “选择安装文件夹”对话框

- ⑤ 单击“下一步”按钮，显示如图9-51所示的“选择开始目录”对话框，并在“开始”菜单中创建快捷方式。

- ⑥ 单击“下一步”按钮，显示如图9-52所示的“选择额外任务”对话框。如果选中“将 Serv-U 作为系统服务安装”复选框，则安装完成以后每次启动系统时，Serv-U 都会自动启动。

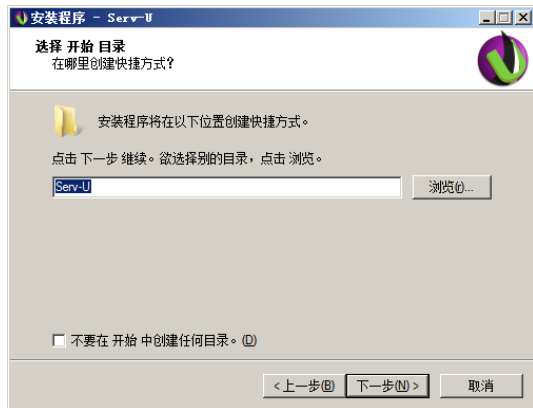


图 9-51 “选择开始目录”对话框

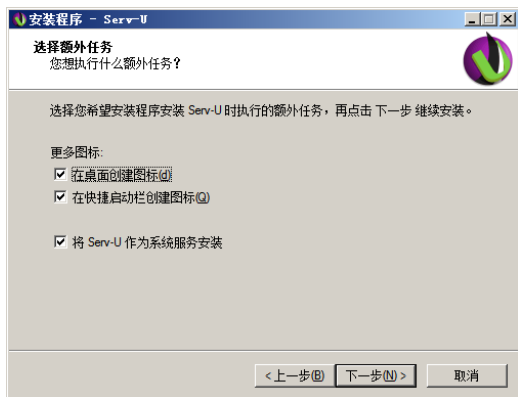


图 9-52 “选择额外任务”对话框

- ⑦ 单击“下一步”按钮，显示如图 9-53 所示的“准备安装”对话框，其中列出前面所做的配置。
- ⑧ 单击“安装”按钮，开始安装。完成后显示如图 9-54 所示的“完成 Serv-U 安装向导”对话框，提示 Serv-U 已安装成功。默认选中“启动 Serv-U 管理控制台”复选框，单击“完成”按钮可自动启动 Serv-U 控制台。



图 9-53 “准备安装”对话框



图 9-54 “完成 Serv-U 安装向导”对话框

2. 使用 Serv-U 配置向导

Serv-U 安装完成在第 1 次启动时会自动启动配置向导，用来创建一个域和用户账户，并为用户指定密码、根目录和权限等信息。

- ① 由于 Windows Server 2008 默认启用“Internet 增强的安全配置”功能，因此当启动 Serv-U 控制台时，首先会显示如图 9-55 所示的“已启用 Windows Internet 增强的安全配置”对话框，提示需要添加信任站点。如果选中“不再显示此提示”复选框，则以后不再显示此对话框。

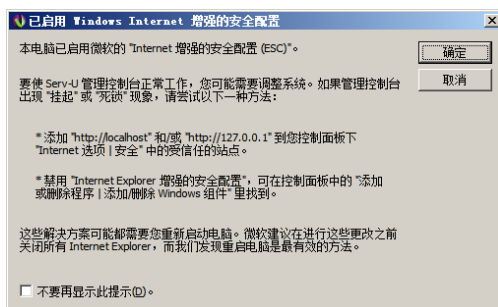


图 9-55 “已启用 Windows Internet 增强的安全配置”对话框

- ② 单击“确定”按钮，提示 http://127.0.0.1 网站已被阻止，如图 9-56 所示。
- ③ 单击“添加”按钮，显示“可信站点”对话框。单击“添加”按钮，将地址 http://127.0.0.1 添加到可信网站列表中，如图 9-57 所示。

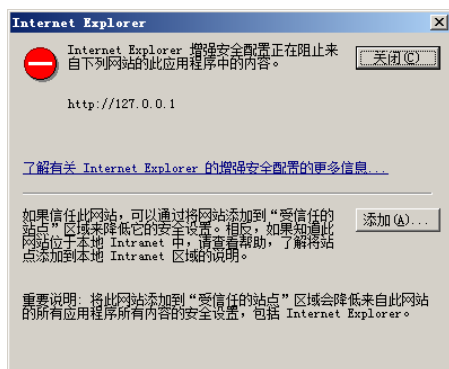


图 9-56 提示信息

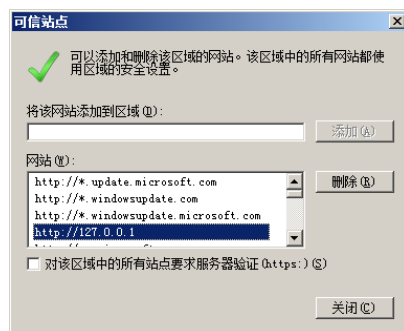


图 9-57 “可信站点”对话框

④ 单击“关闭”按钮，启动如图 9-58 所示的 Serv-U 控制台。由于尚未创建域。因此会提示是否要定义新域。



图 9-58 Serv-U 控制台

⑤ 单击“是”按钮，显示如图 9-59 所示的“域向导”对话框。在“名称”文本框中键入新域的名称，选中“启用域”复选框以启用域。

⑥ 单击“下一步”按钮，显示如图 9-60 所示的域向导之二。提示可使用域提供多种协议的发布，选择要安装协议相应的复选框。

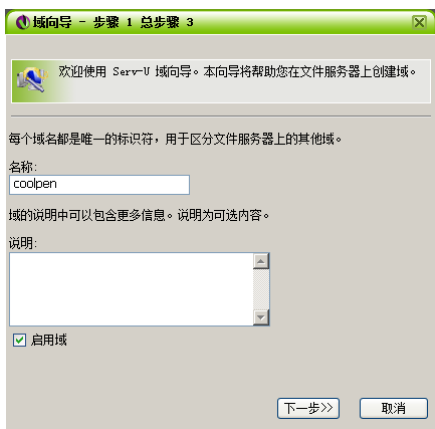


图 9-59 “域向导”对话框

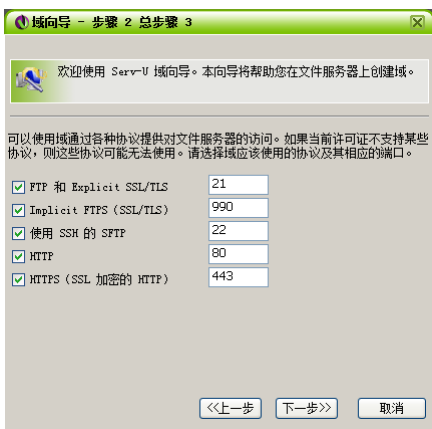


图 9-60 域向导之二

⑦ 单击“下一步”按钮，显示如图 9-61 所示的域向导之三，在“IP 地址”文本框中为当前域键入 IP 地址。如果保留为空，则表示使用当前计算机上的所有 IP 地址。

⑧ 单击“完成”按钮，显示如图 9-62 所示的提示框，提示是否要为域创建用户账户。

⑨ 单击“是”按钮，显示如图 9-63 所示的提示框，提示是否要使用向导创建用户。

⑩ 单击“是”按钮，显示如图 9-64 所示的“用户向导”之一，在“用户名”文本框中键入待创建的用户账户名。

⑪ 单击“下一步”按钮，显示用户向导之二。在“密码”文本框中为新用户设置密码，如图 9-65 所示。

⑫ 单击“下一步”按钮，显示如图 9-66 所示的用户向导之三，在其中设置用户的根目录。默认选中“锁定用户至根目录”复选框，将匿名用户限制在其主目录。使其只访问用户所登录的主目录，无法访问主目录之外的内容。

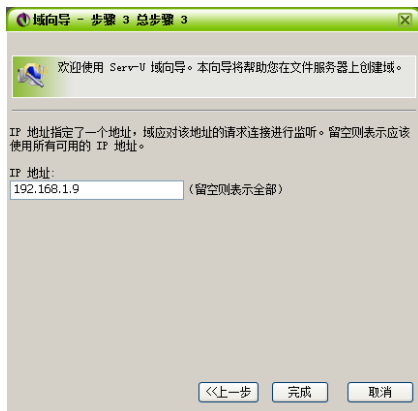


图 9-61 域向导之三

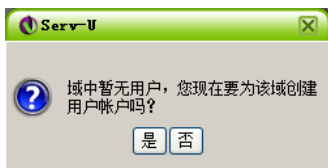


图 9-62 提示框

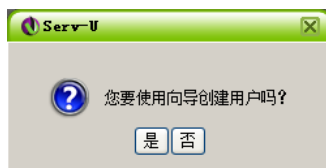


图 9-63 提示框

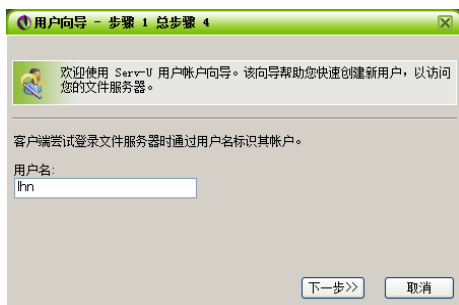


图 9-64 “用户向导”之一

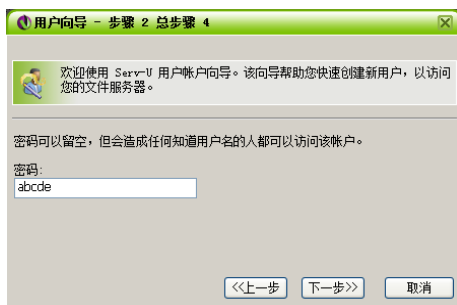


图 9-65 设置用户密码

⑬ 单击“浏览”按钮，显示如图 9-67 所示的“浏览”对话框，为新用户选择根目录所在的文件夹。

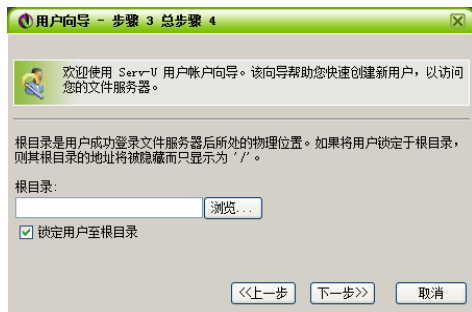


图 9-66 用户向导之三

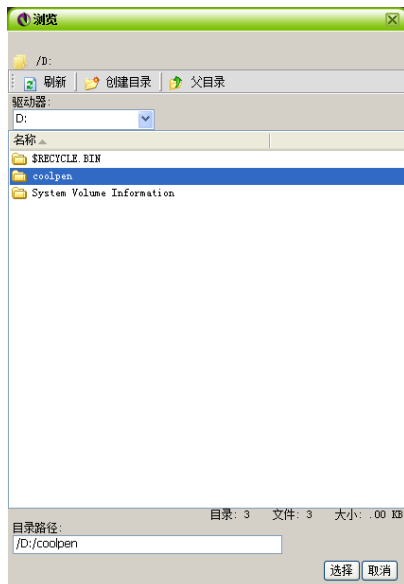


图 9-67 “浏览”对话框

14 单击“下一步”按钮，显示如图 9-68 所示的用户向导之四。在“访问权限”下拉列表框中选择访问权限，包括“只读访问”和“完全访问”两种权限。

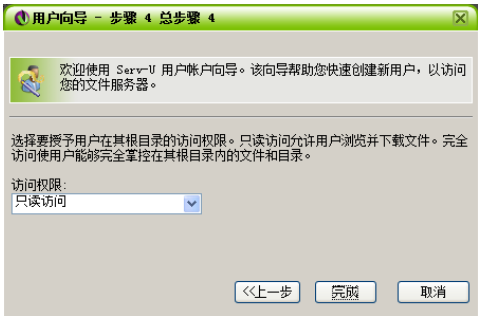


图 9-68 用户向导之四

15 单击“完成”按钮，用户创建完成。并显示在如图 9-69 所示的“用户”窗口中。所有用户的配置都可在该窗口中完成。

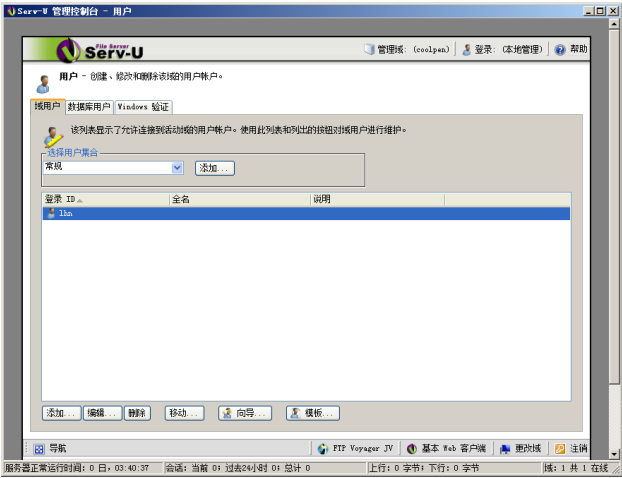


图 9-69 “用户”窗口

至此，在 Serv-U 中创建一个域和一个用户账户，客户利用该账户即可访问 FTP 服务器。在窗口下方，将鼠标移动到“导航”，在快捷菜单中单击“主页”选项，显示“Serv-U 管理控制台 - 主页”窗口，如图 9-70 所示，在其中即可管理域及用户等所有设置。



图 9-70 “Serv-U 管理控制台 - 主页”窗口

提示

在每个设置页面都可以单击“导航”中的“主页”选项来返回 Serv-U 主页。

9.5.2 管理用户和权限

在安装 Serv-U 时可利用向导创建一个域和用户，在安装以后也可以创建其他用户，并为每个用户设置欢迎消息、访问权限及访问目录等。

1. 添加用户账户

① 单击“开始”→“程序”→“Serv-U”→“Serv-U 管理控制台”选项，或者在桌面托盘区域中右击 Serv-U 图标，选择快捷菜单中的“启动管理控制台”选项，打开“Serv-U 管理控制台 - 主页”窗口。

② 单击“用户”超级链接，显示如图 9-71 所示的“用户”窗口，在安装 Serv-U 时已经利用向导创建了一个用户。

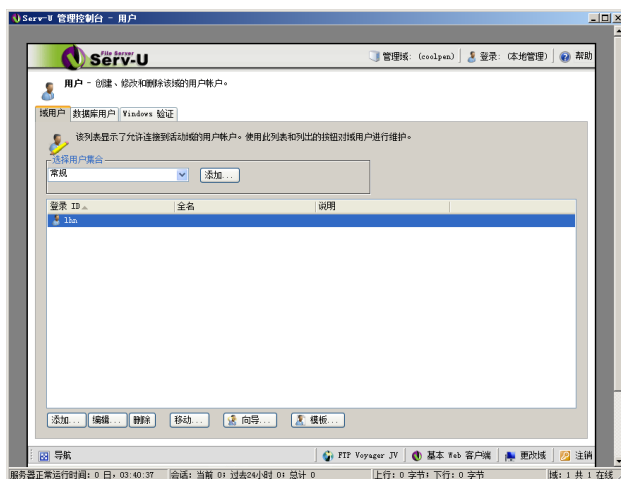


图 9-71 “用户”窗口

提示



如果单击“向导”按钮，则可启用用户向导来创建用户，操作过程和安装 Serv-U 时启用的向导一样。

③ 如果要添加一个用户，则单击“添加”按钮，显示如图 9-72 所示的“用户属性”对话框。

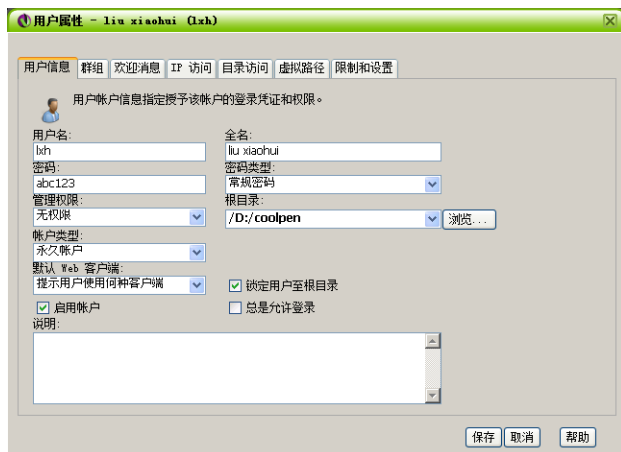


图 9-72 “用户属性”对话框

在其中设置如下选项。

用户名：键入要添加的用户名称。

全名：设置新用户的全名。

密码：为新用户设置一个密码，使用“密码类型”下拉列表框中的“常规密码”即可。

管理权限：设置新用户的管理权限，默认为“无权限”，也可以设置“域管理员”或“系统管理员”权限。

根目录：指定可访问的根目录。

账户类型：设置新用户账户的类型，默认为永久账户。选择“自动禁用”选项则禁用该账户，选择“自动删除”选项则可删除该账户。

(4) 单击“保存”按钮，该用户添加成功。按照同样操作步骤可添加多个用户。

2. 设置欢迎消息

“欢迎消息”用于设置用户登录到 FTP 服务器时显示的欢迎消息。

① 在“用户”窗口中选择待设置欢迎消息的用户，单击“编辑”按钮，显示如图 9-73 所示的“用户属性”对话框。默认为“用户信息”选项卡，在其中可以设置用户名、密码及根目录等信息。

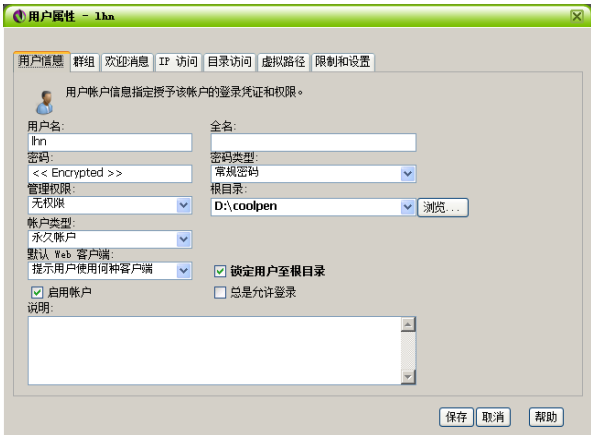


图 9-73 “用户属性”对话框

② 打开“欢迎消息”选项卡，如图 9-74 所示。Serv-U 支持使用消息文件，如果事先编辑了欢迎消息文件，则单击“浏览”按钮选择该文件。如果不使用消息文件，必须选中“使用定制的欢迎消息覆盖继承的群组欢迎消息”复选框，然后直接在文本框中设置消息文件内容。

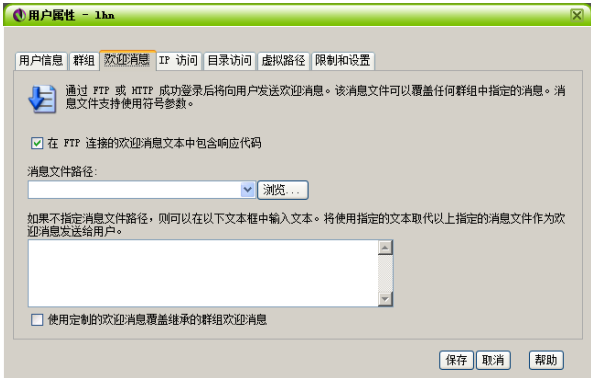


图 9-74 “欢迎消息”选项卡

3. IP 访问限制

“IP 访问”选项卡用于设置限制允许或拒绝访问服务器的 IP 地址或 IP 地址段，从而保护 FTP 服

服务器的安全。

① 在“用户属性”对话框中打开如图 9-75 所示的“IP 访问”选项卡，在其中设置限制用户的 IP 地址。

② 单击“添加”按钮，显示如图 9-76 所示的“IP 访问规则”对话框。如果要允许特定 IP 地址访问 FTP 服务器，则选择“允许访问”单选按钮；如果要拒绝，则选择“拒绝访问”单选按钮，然后在文本框中键入允许或拒绝访问的 IP 地址或 IP 地址段。

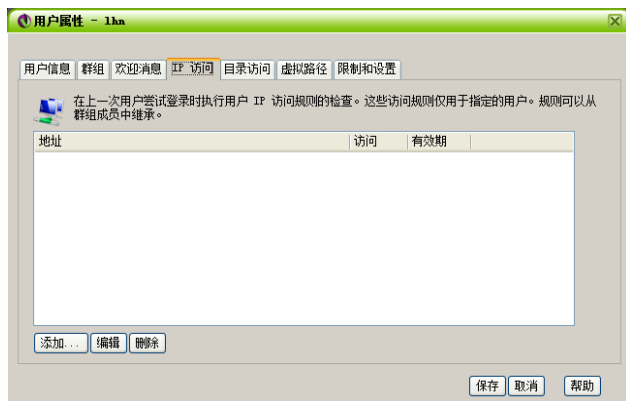


图 9-75 “IP 访问”选项卡

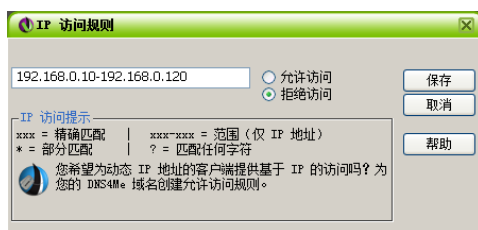


图 9-76 “IP 访问规则”对话框



提示

可以使用通配符 (*、? 及-) 来限制 IP 地址，其中“*”匹配所有字符；“?”只匹配单个字符。例如 192.168.0.*，将拒绝 192.168.0.1~192.168.0.254 IP 地址段的访问；192.168.0.? 将拒绝 192.168.0.1~192.168.0.9 IP 的访问。192.168.0.1-192.168.0.50 将限制该段 IP 地址。

③ 单击“保存”按钮，添加成功限制的 IP 地址。按照同样操作步骤可添加多个 IP 地址或 IP 地址段，如图 9-77 所示。

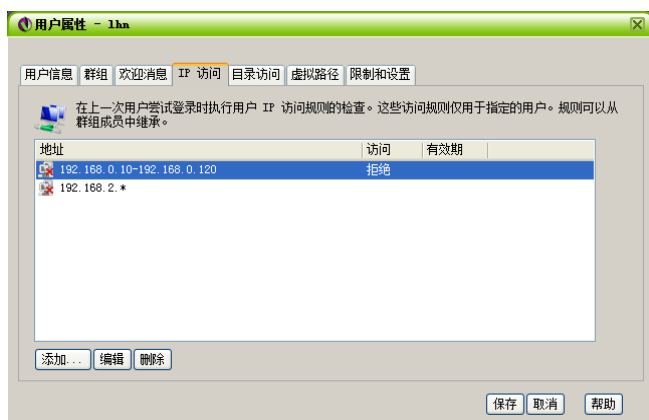


图 9-77 限制的 IP 地址

4. 限制目录访问

“目录访问”选项卡用于设置用户可以访问的文件和目录，虽然添加用户时已经为用户设置了根目录，但也可以为其添加多个允许访问的目录。

① 在“用户属性”对话框中打开“目录访问”选项卡，如图 9-78 所示，其中“%HOME%”目录是添加用户时设置的根目录。

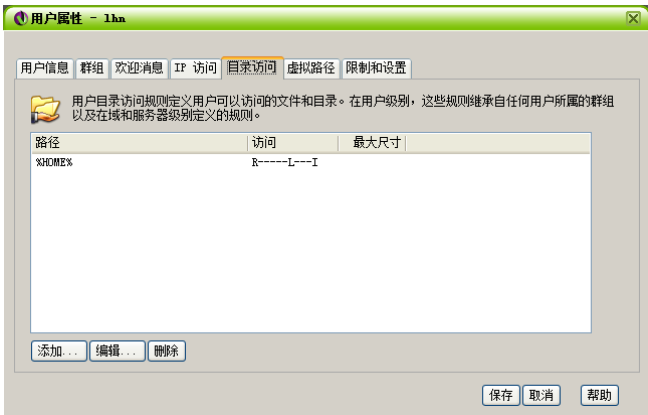


图 9-78 “目录访问”选项卡

② 单击“添加”按钮，显示如图 9-79 所示的“目录访问规则”对话框，设置如下选项。

路径：键入允许用户访问的目录路径，或者单击“浏览”按钮选择。

文件：设置用户访问目录中文件的权限。

目录：设置用户访问目录的权限。

子目录：如果选中“继承”复选框，则为父目录设置的权限自动应用到子目录上。

目录内容的最大尺寸：设置允许用户上传文件的最大容量，即磁盘配额功能。

单击“完全访问”按钮，可选中所有复选框，从而赋予完全访问权限；单击“只读”按钮，则只赋予只读访问权限。

③ 单击“保存”按钮，添加成功一个目录（如图 9-80 所示），用户即可访问该目录中的内容。按照同样步骤，可以为用户添加多个目录。选中一个目录，单击“编辑”按钮则可修改该目录的设置；单击“删除”按钮则可删除该目录。



图 9-79 “目录访问规则”对话框

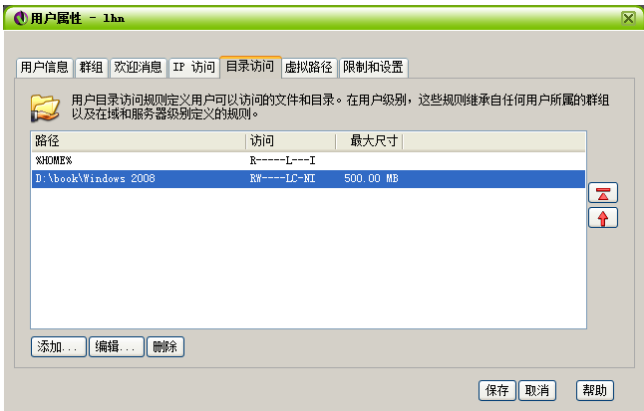


图 9-80 添加成功一个目录

5. 限制和设置

“限制和设置”选项卡用来设置限制用户的连接数量、密码类型、目录列表类型和传输速度等。默认状态下，Serv-U 并没有对用户进行限制，需要用户根据实际需要添加相应的限制选项。

① 在“用户属性”对话框中打开如图 9-81 所示的“限制和设置”选项卡，在“限制类型”下拉列表框中默认为“连接”选项，可以限制每个用户或 IP 地址的最大连接数量。如果要显示其他限制或设置，则在“限制类型”下拉列表框中选择相应的选项。

② 要添加一项限制规则，可单击“添加”按钮，显示如图 9-82 所示的“限制”对话框。在“限制”下拉列表框中选择要限制选项，例如“每个用户账户连接的最大会话数”。然后在“每个用户账户连接的最大会话数”文本框中键入限制的数量，如 10。



图 9-81 “限制和设置”选项卡

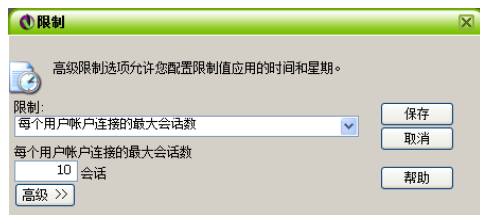


图 9-82 “限制”对话框

③ 如果要设置该限制应用时间，则单击“高级”按钮，显示的高级设置选项如图 9-83 所示，在“时间”和“星期”选项区域中设置限制时间即可。

④ 单击“保存”按钮保存设置，如图 9-84 所示，按照同样步骤可继续添加其他限制选项。

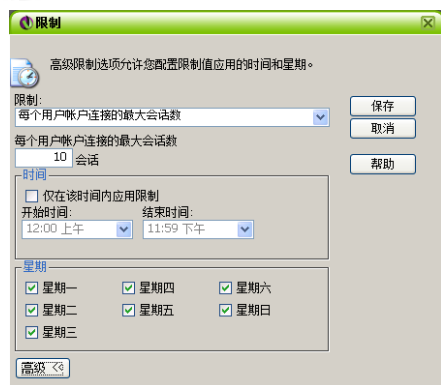


图 9-83 高级设置选项

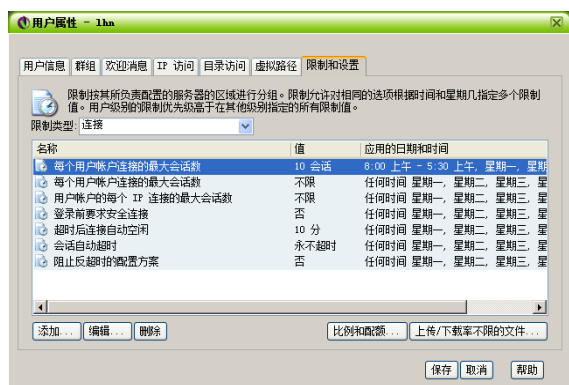


图 9-84 添加限制选项

9.5.3 管理域

在 Serv-U 中的每个域相当于一台服务器，用来管理 FTP 站点和用户。在 Serv-U 中可以添加多个域，每个域可以添加多个用户。在安装 Serv-U 后可以根据系统提示，利用向导创建一个域。如果没有创建域，则可以在安装完成后添加。

1. 添加和删除域

(1) 单击“开始”→“程序”→“Serv-U”→“Serv-U 管理控制台”选项，或者在桌面托盘区域中右击 Serv-U 图标，选择快捷菜单中的“启动管理控制台”选项，打开“Serv-U 管理控制台 - 主页”窗口。

(2) 单击窗口上方的“新建域”按钮，显示如图 9-85 所示的“域向导”对话框。利用该向导可创建新域，并在其中添加用户账户。具体操作和安装 Serv-U 后启动的向导一样，请参见前面所述内容，这里不再赘述。

如果在 Serv-U 中创建了多个域，要从当前域切换到其他域，则单击“管理域”按钮，或者单击窗口下方的“更改域”按钮，显示如图 9-86 所示的“域”对话框。选择要管理的域，单击“选择”按钮即可登录。如果要删除某个域，单击“删除”按钮即可。

2. 查看活动状态

在 Serv-U 中可以查看某个域，或者 FTP 服务器有哪些用户正在连接，以及各用户文件的传输速度等，从而可以清楚地了解 FTP 服务的使用情况。

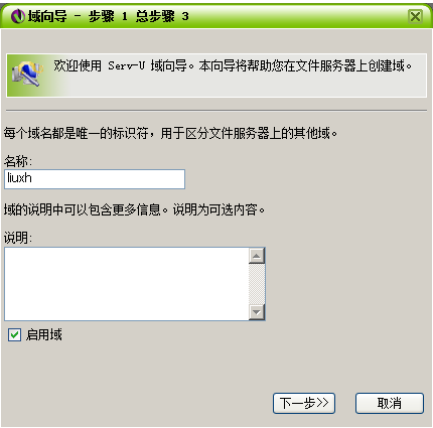


图 9-85 “域向导” 对话框

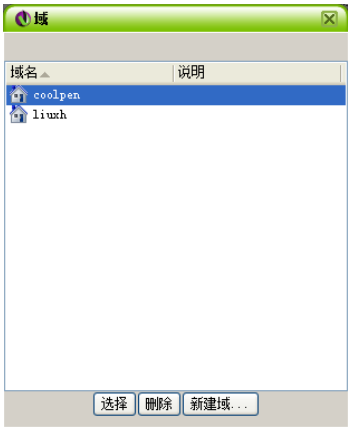


图 9-86 “域” 对话框

在 Serv-U 控制台主页中，单击“域活动”超级链接，显示如图 9-87 所示的“域活动”窗口。其中显示当前连接到该域的所有用户的活动信息，包括访问的 FTP 目录、客户端 IP 地址及传输速度等。在其中还可以断开或者中断某个用户的连接。

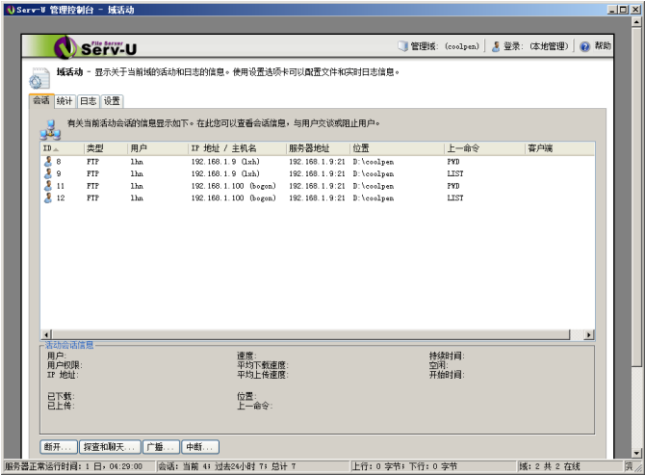


图 9-87 “域活动” 窗口

在 Serv-U 控制台主页中单击“服务器活动”超级链接，显示如图 9-88 所示的“服务器活动”窗口。在其中可以查看所有连接到当前服务器的用户，包括所有域的活动信息。

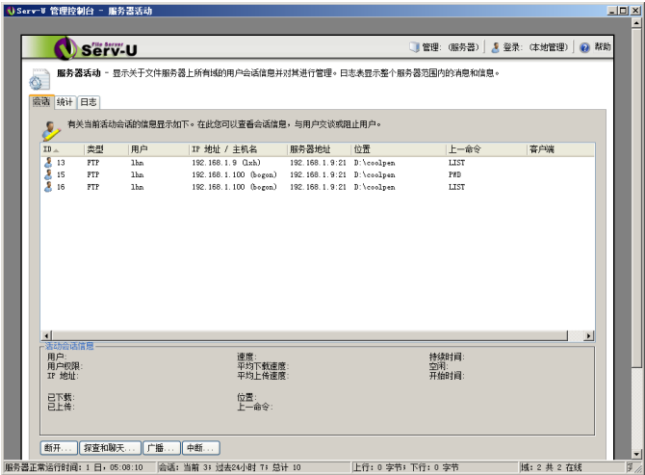


图 9-88 “服务器活动” 窗口

9.6 使用 FTP 客户端

当 FTP 服务器架设成功以后,即可为用户提供文件上传和下载服务。根据 FTP 站点所设置的权限不同,用户访问 FTP 目录中文件的权限也不一样。访问 FTP 网站一般使用两种方式,一是利用 Windows 资源管理器;二是利用专门的 FTP 客户端软件。

9.6.1 访问 FTP 站点

如果 FTP 网站启用了匿名访问,用户可以直接访问 FTP 网站,而无须输入用户名和密码;如果 FTP 网站禁用了匿名访问,用户则必须输入 FTP 服务器或域中具有访问权限的用户名和密码。

1. 利用 Windows 资源管理器访问

打开 Windows 资源管理器,在地址栏中输入 FTP 站点的访问地址,格式为:

`ftp://服务器名或 IP 地址/目录名`

例如,输入 `ftp://ftp.coolpen.net` 或 `ftp://192.168.1.8`,按回车键。如果该 FTP 网站启用了匿名访问,那么可以连接 FTP 服务器并显示其中的文件和文件夹,如图 9-89 所示。

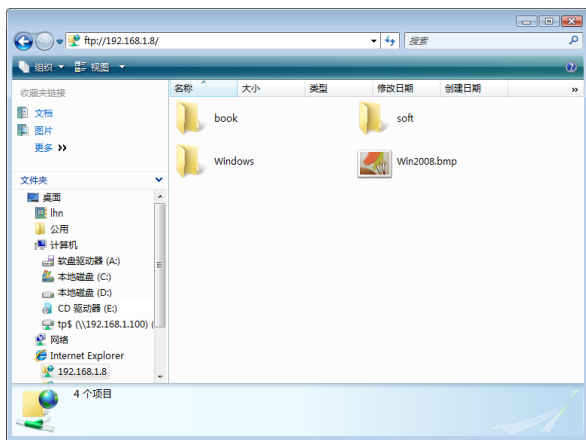


图 9-89 访问 FTP 站点

如果 FTP 网站禁用了匿名访问,那么连接到 FTP 服务时就会显示如图 9-90 所示的“登录身份”对话框。在“用户名”和“密码”文本框中键入 FTP 服务器或域中的用户账户名和密码,单击“登录”按钮即可登录到 FTP 服务器。

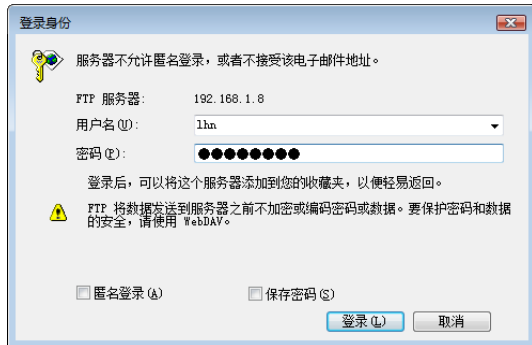


图 9-90 “登录身份”对话框

也可以在 Windows 资源管理器的地址栏中直接输入 `ftp://用户名:密码@FTP 服务器地址` 来登录到 FTP 服务器,例如, `ftp://lhn:abcdef@192.168.1.8`。选择可直接登录 FTP 服务器,而不再显示“登录身份”对话框。

如果用户登录到 FTP 服务器后要使用其他用户账户登录,可右击空白处,选择快捷菜单中的“登录”选项,显示“登录身份”对话框。键入用户名和密码,单击“登录”按钮即可。

用户登录到 FTP 服务器后可以根据 FTP 服务器所设置的权限读取或写入数据,并且操作方式和在 Windows 中复制和粘贴文件一样。

(1) 从 FTP 站点中下载文件时,选择要下载的文件。右击并选择快捷菜单中的“复制”选项,然后打开 Windows 资源管理器,粘贴到要保存的位置即可。

(2) 如果用户具有“写入”权限,要上传文件,可在 Windows 资源管理器中复制文件,然后粘贴到 FTP 网站文件夹中即可。

具有“写入”权限时,还可以更改文件或文件夹名、删除文件和文件夹。登录到 FTP 网站以后,选择待删除或重命名的文件或文件夹,右击并选择快捷菜单中的“删除”或“重命名”选项。如果要新建文件夹,可右击 FTP 窗口的空白处,选择快捷菜单中的“新建”→“文件夹”选项。

2. 利用 FTP 软件访问

现在有很多专门用于访问 FTP 服务器的软件,如 CuteFTP 及 FlashFXP 等,用户可从 Internet 中下载。这里以 CuteFTP 为例介绍。

运行 CuteFTP 程序,在工具栏中的“Host”文本框中键入 FTP 服务器的地址,在“Username”文本框中键入用户名,在“Password”文本框中键入密码。单击“Connect”按钮或按回车键,登录到 FTP 服务器。显示 FTP 服务器中的文件及文件夹,如图 9-91 所示。

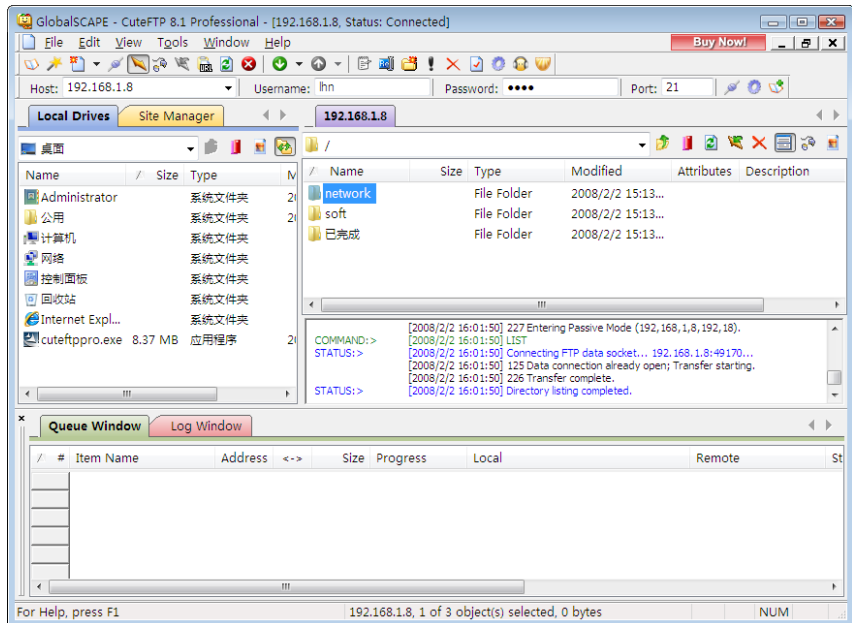


图 9-91 FTP 服务器中的文件及文件夹

如果要从 FTP 服务器下载文件,则在“Local Drives”列表框中打开要保存的文件夹。然后在 FTP 站点列表中选择要下载的文件,右击并选择快捷菜单中的“Download”选项即可将文件下载到本地。

如果要向 FTP 服务器上传文件,则在 FTP 站点列表框中打开保存上传文件的文件夹。然后在“Local Drives”列表框中选择要上传的文件,右击并选择快捷菜单中的“Upload”选项即可将文件上传到 FTP 服务器。

如果要重命名 FTP 站点中的文件,则右击并选择快捷菜单中的“Rename”选项,键入一个新名称即可;如果要删除文件,则选择快捷菜单中的“Delete”选项。显示如图 9-92 所示的提示框,单击“是”按钮即可删除。

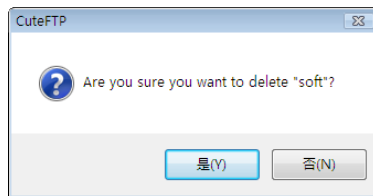


图 9-92 提示框

9.6.2 访问虚拟目录

如果要访问 FTP 站点中的虚拟目录，只需在要访问的 FTP 地址中加上虚拟目录名即可，格式为：

`ftp://FTP 服务器名或 IP 地址/虚拟目录名`

或者：

`ftp://用户名:密码@FTP 服务器名或 IP 地址/虚拟目录名`

例如：

`ftpo://192.168.1.8/book`

或者：

`ftp://192.168.1.8/lhn:abcdef@192.168.1.8/books`

第 10 章 配置与管理文件服务

资源共享是网络最大的特点之一，而局域网的资源共享更多的是借助文件共享来实现。文件服务是局域网中很常用的网络服务之一，通常利用文件服务器的 RAID 卡和高速的 SCSI 硬盘为网络提供文件共享。还可以设置网络文件的保护权限，在高速存取的同时确保了访问的安全，也能够充分利用大容量的磁盘存储空间。

10.1 文件共享与 NTFS 权限

为了保护数据存储的安全，并且避免由于硬盘损坏造成的数据丢失，通常为文件服务器配置有 RAID 卡和高速的大容量硬盘，为网络中的用户提供文件共享。同时通过设置严格的权限策略，在保证为网络提供文件共享的同时，也要保证数据的访问安全。

10.1.1 设置文件夹共享

文件共享是 Windows Server 2008 系统内置的功能，不需安装文件服务即可使用，在 Windows 资源管理器、文件服务器及控制台中均可设置文件共享。

1. 在 Windows 资源管理器中设置

在 Windows 资源管理器中可以将文件夹设置为共享，操作非常简单，而且可以使用简单共享和高级共享。简单共享只能设置允许访问共享的用户账户，以及简单的访问权限；而高级共享不仅可以设置访问用户，而且可以设置连接数、共享名及脱机访问等。

设置简单共享的操作步骤如下。

① 打开 Windows 资源管理器，选择要设置共享或者已经设置为共享的文件夹。右击并选择快捷菜单中的“共享”选项，显示如图 10-1 所示的“文件共享”对话框。

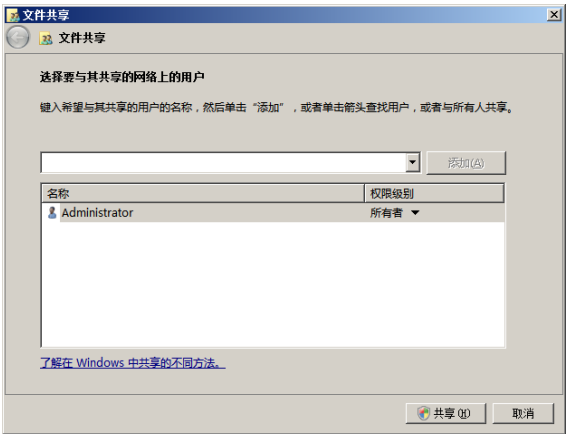


图 10-1 “文件共享”对话框

② 在下拉列表框中选择允许访问该共享的用户账户，例如选择“Everyone”账户以允许所有用户访问。单击“添加”按钮将该用户添加到下方的用户列表框中，如图 10-2 所示。右击用户名，可在快捷菜单中为该用户账户选择访问权限，包括读者、参与者和共有者，相当于读取、更改和完全控制权。选择“删除”选项，则可删除该用户账户。



图 10-2 设置用户访问权限

③ 设置完成后单击“共享”按钮，该文件夹被共享，如图 10-3 所示。单击“完成”按钮完成共享。



图 10-3 文件夹被共享

设置高级共享的操作步骤如下。

① 在 Windows 资源管理器中选择要共享的文件夹，右击并选择快捷菜单中的“属性”选项。打开文件夹属性对话框，打开“共享”选项卡，如图 10-4 所示。单击“共享”按钮，可以利用简单共享设置。

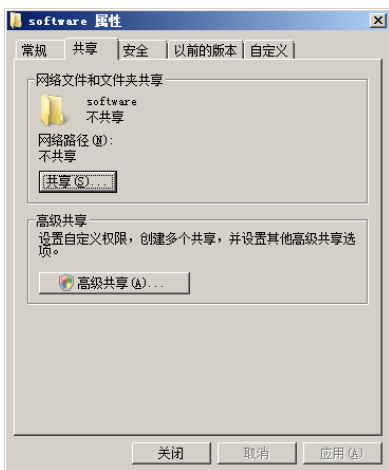


图 10-4 “共享”选项卡

② 单击“高级共享”按钮，显示如图 10-5 所示的“高级共享”对话框，选中“共享此文件夹”复选框即可共享此文件夹。在“共享名”文本框中可设置共享名称，在“将同时共享的用户数量限制为”文本框中设置同时连接的数量。

③ 单击“权限”按钮，显示所选文件夹的权限对话框，用来设置访问权限。默认已添加了“Everyone”账户，且为“读取”权限。可单击“添加”按钮添加允许访问共享文件夹的用户账户，并在权限列表框中选择权限，如图 10-6 所示。

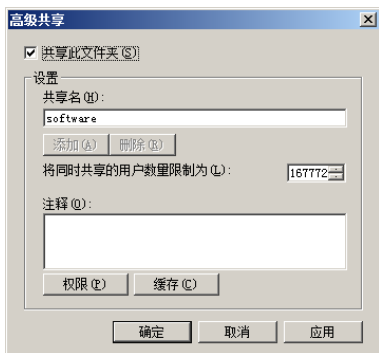


图 10-5 “高级共享”对话框

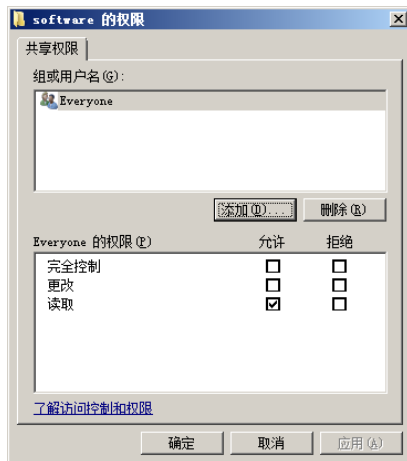


图 10-6 设置权限

④ 设置完成以后，依次单击“确定”按钮，所选文件夹被设置为共享。

2. 在文件服务器中设置

① 打开“服务器管理器”窗口，依次展开“角色”→“文件服务”→“共享和存储管理”选项。显示如图 10-7 所示的“共享和存储管理”窗口，其中列出系统当前所有共享的文件夹。

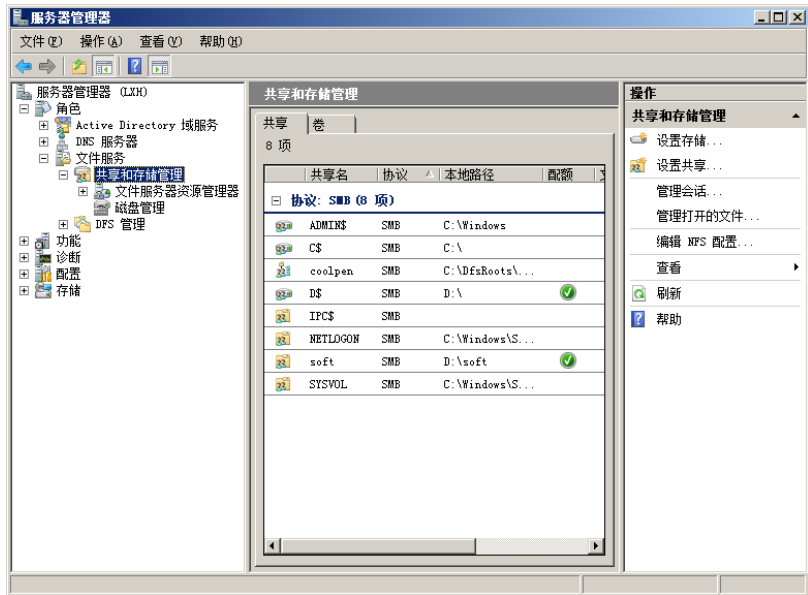


图 10-7 “共享和存储管理”窗口

② 在左侧的“操作”窗格中单击“设置共享”超级链接，显示“共享文件夹位置”对话框，如图 10-8 所示。

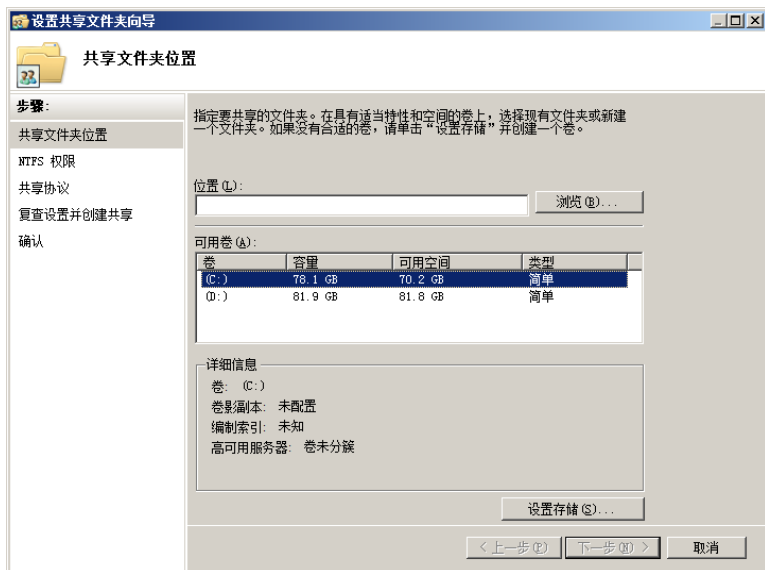


图 10-8 “共享文件夹位置”对话框

③ 在“位置”文本框中键入文件夹路径，或者单击“浏览”按钮，显示如图 10-9 所示“浏览文件夹”对话框。在本地磁盘中选择一个要设置为共享的文件夹，单击“确定”按钮即可。



提示

磁盘分区必须已被设置为系统默认共享时，才能在此处选择其中的文件夹。而新划分的分区可能会因尚未设置为系统分享而无法选择，此时重新启动系统即可。



图 10-9 “浏览文件夹”对话框

④ 系统自动格式化新创建的卷，单击“下一步”按钮，显示如图 10-10 所示的“NTFS 权限”对话框。指定 NTFS 权限以控制具体用户和组如何在本地访问该文件夹，网络中的用户访问该文件夹时会以其所登录的用户权限来访问该文件夹。选择“否，不更改 NTFS 权限”单选按钮，将会以该文件夹自己的 NTFS 设置来控制允许访问的用户；选择“是，更改 NTFS 权限”单选按钮，并单击“编辑权限”按钮即可根据需要设置该文件夹的访问权限。

⑤ 单击“下一步”按钮，显示如图 10-11 所示的“共享协议”对话框。根据需要选择可访问该共享文件夹的协议，这里选中“SMB”复选框。在“共享名”文本框中键入共享文件夹名称，在“共享路径”文本框中设置其网络路径。

⑥ 单击“下一步”按钮，显示如图 10-12 所示的“SMB 设置”对话框。指定客户端如何通过 SMB 协议访问此文件夹，用户可以通过在描述中添加如何使用该共享文件夹等信息。在“高级设置”选项组中可以设置允许最大的连接数、基于访问权限的枚举和脱机设置。



图 10-10 “NTFS 权限”对话框



图 10-11 “共享协议”对话框



图 10-12 “SMB 设置”对话框

⑦ 单击“高级”按钮，显示如图 10-13 所示的“高级”对话框。如果服务器的性能不是很好的话，可以在这里限制同时访问该服务器的用户数量，从而达到减小服务器负荷的目的。选中“允许此数量的用户”单选按钮，并在文本框键入待设置的用户数量。选中“启用基于访问权限的枚举”复选框，可以根据具体用户的访问权限筛选用户可以看到的共享文件夹，从而避免显示用户无权访问的文件夹和其他共享资源。

⑧ 打开“缓存”选项卡，如图 10-14 所示。设置允许用户访问的共享内容，以及如何使用。

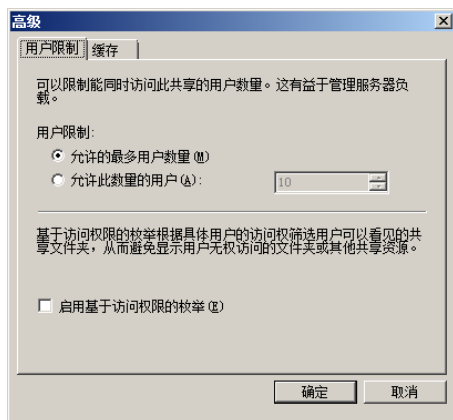


图 10-13 “高级”对话框

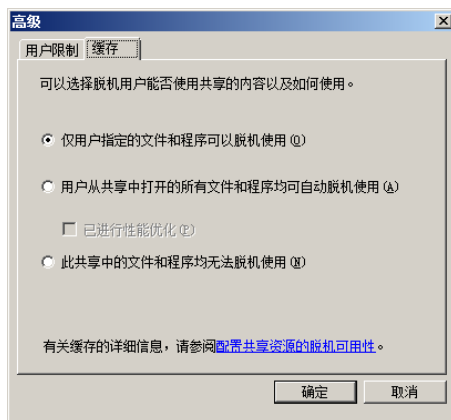


图 10-14 “缓存”选项卡

在其中设置如下内容。

只允许用户访问和使用指定的文件和程序。

允许用户访问和使用所有共享中的文件和程序。

禁止用户访问和使用共享中的所有文件和程序。

⑨ 单击“确定”按钮，返回“SMB 设置”对话框。单击“下一步”按钮，显示如图 10-15 所示的“SMB 权限”对话框。

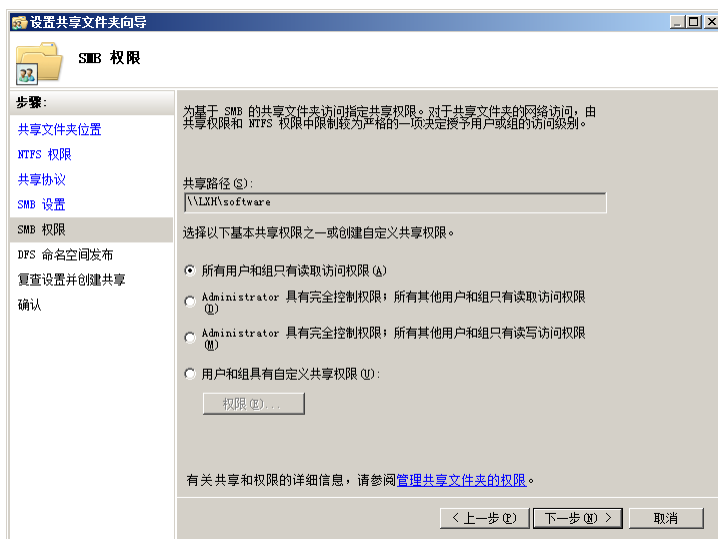


图 10-15 “SMB 权限”对话框

设置该共享文件夹的基本共享权限。

所有用户和组只有读取访问权限。

Administrator 具有“完全控制”权限，所有其他用户和组只有读取访问权限。

Administrator 具有“完全控制”权限，所有其他用户和组只有读写访问权限。

用户和组具有自定义共享权限。

⑩ 单击“下一步”按钮，显示如图 10-16 所示的“配额策略”对话框，在其中设置配额以限制此共享文件夹的最大容量。

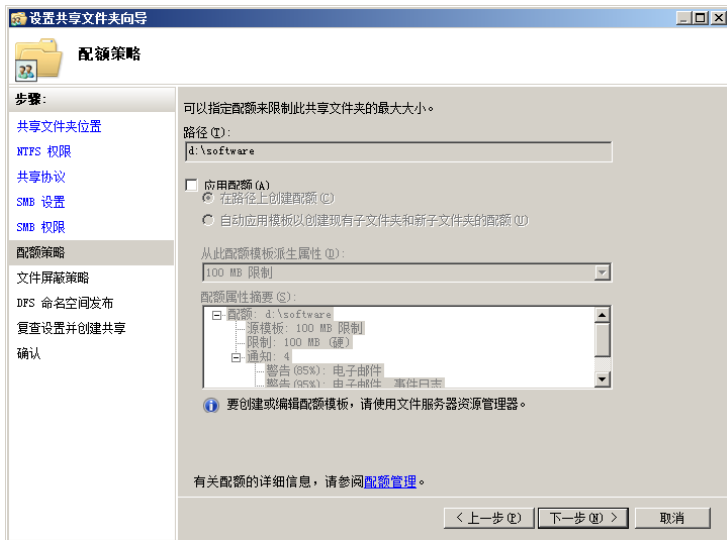


图 10-16 “配额策略”对话框

⑪ 单击“下一步”按钮，显示如图 10-17 所示的“文件屏蔽策略”对话框，在其中设置是否对共享文件夹应用文件屏蔽。

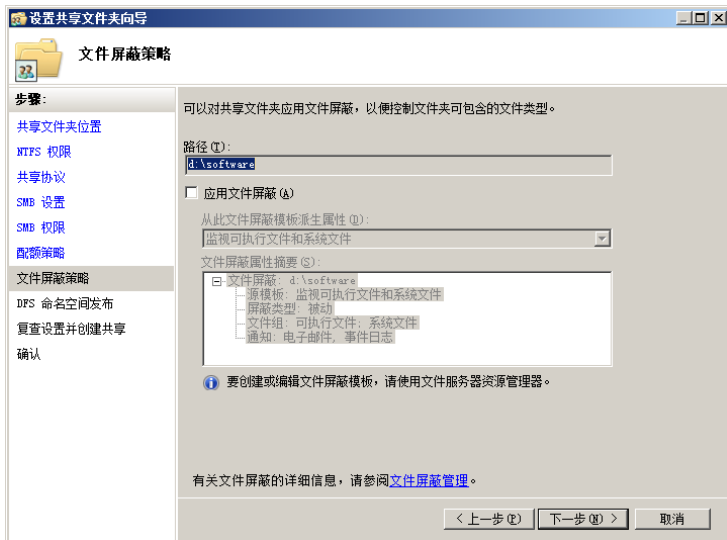


图 10-17 “文件屏蔽策略”对话框

⑫ 单击“下一步”按钮，显示如图 10-18 所示的“DFS 命名空间发布”对话框。在其中将共享文件夹发布到现有的 DFS 命名空间，也可以以后再发布。

⑬ 单击“下一步”按钮，显示如图 10-19 所示的“复查设置并创建共享”对话框。在共享文件夹设置中检查前面所做的设置是否正确，单击“上一步”按钮，可返回重新设置。

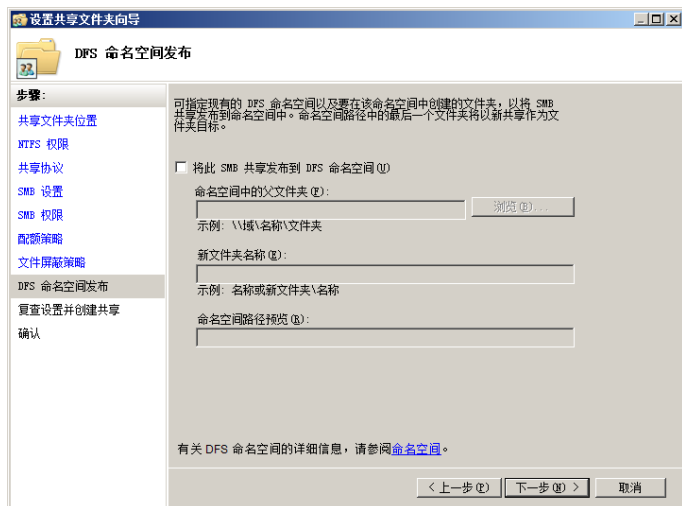


图 10-18 “DFS 命名空间发布”对话框



图 10-19 “复查设置并创建共享”对话框

⑭ 单击“创建”按钮，系统开始创建操作，创建成功后显示如图 10-20 所示的“确认”对话框。单击“关闭”按钮，完成在文件服务器中设置共享的操作，新创建的共享即可显示在“服务器管理器”窗口中。



图 10-20 “确认”对话框

⑮ 单击“关闭”按钮，创建完成共享文件夹，如图 10-21 所示。按照同样步骤，可以设置多个共享文件夹。

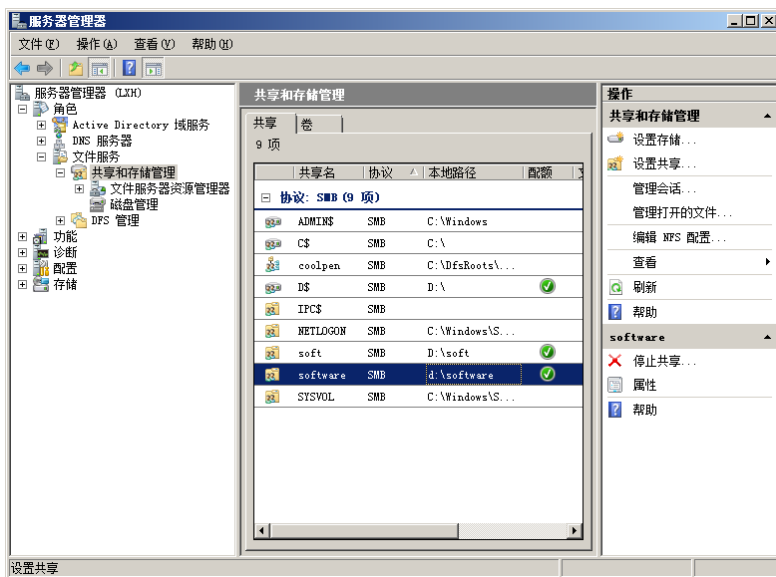


图 10-21 创建完成共享文件夹

10.1.2 NTFS 权限

NTFS 是从 Windows NT 开始引入的文件系统，借助于 NTFS 不仅可以为文件夹授权，而且还可以为单个文件授权，使得对用户访问权限的控制变得更加细致。NTFS 还支持数据压缩和磁盘限额，从而可以进一步高效率地使用硬盘空间。除此之外，它还可对文件系统进行透明加密，从而使保存的文件数据更加安全。因此服务器应当采用 NTFS 文件系统，以实现对资源的安全访问。

利用 NTFS 权限可以控制用户账户和组对文件夹和文件的访问，当然该权限只适用于 NTFS 磁盘分区，而不能用于 FAT 或 FAT32 文件系统。Windows Server 2008 只为用 NTFS 格式化的磁盘分区提供 NTFS 权限，为了保护 NTFS 磁盘分区中的文件和文件夹，需要为访问该资源的每一个用户账户授予 NTFS 权限。用户账户必须获得明确的授权才能访问资源，如果没有被组授予权限，则不能访问相应的文件或文件夹。

注意：

无论用户访问文件夹还是访问文件，也无论这些文件夹或文件是在计算机上，还是在网络上，NTFS 的安全性功能都有效。即无论是以用户身份登录到服务器，还是通过网络访问共享文件夹，NTFS 安全性都有效。因此从安全性角度考虑，在准备共享文件夹之前必须设置其 NTFS 权限。



对于 NTFS 分区中的每一个文件和文件夹，NTFS 都存储一个远程访问控制列表（ACL），其中包含那些被授权访问该文件或者文件夹的所有用户账户、组和计算机，及其被授予的访问类型。为了让一个用户访问某个文件或文件夹，针对相应的用户账户、组，或者该用户所属的计算机，ACL 中必须包含一个对应的元素，叫做“访问控制元素”（ACE）。为了让用户能够访问文件或者文件夹，访问控制元素必须具有用户所请求的访问类型。如果 ACL 中没有相应的 ACE 存在，则会拒绝该用户访问相应资源。



1. NTFS 权限的类型

在 NTFS 分区中，可以分别为文件与文件夹的设置 NTFS 权限。不过尽量不要采用直接为文件设置权限的方式，最好是将文件放置于文件夹中，然后设置其权限。

NTFS 文件权限有以下类型。

- (1) 读取：可以读该文件的数据、查看文件属性、查看文件的所有者及权限。
- (2) 写入：可以更改或覆盖文件的内容，更改文件属性并查看文件的所有者及权限。
- (3) 读取及运行：拥有“读取”的所有权限，还具有运行应用程序的权限。
- (4) 修改：拥有“读取”、“写入”权限和“读取及运行”的所有权限，并可以修改和删除文件。
- (5) 完全控制：拥有所有的 NTFS 文件权限，不仅具有上述所有权限，还具有更改权限和取得所有权的权限。

NTFS 文件夹权限有以下类型。

- (1) 读取：可以查看该文件夹中的文件和子文件夹，查看文件夹的所有者、属性（如只读、隐藏、存档和系统）及其权限。
- (2) 写入：可以在文件夹内添加文件和子文件夹、更改文件夹属性、查看文件夹的所有者及其权限。
- (3) 列出文件夹目录：具有拥有“读取”的所有权限，以及“遍历子文件夹”的权限，即具备进入到子文件夹的功能。
- (4) 读取及运行：拥有“读取”权限和“列出文件夹目录”权限的所有权限，“列出文件夹目录”的权限仅由文件夹继承；“读取和运行”权限是由文件夹和文件同时继承。
- (5) 修改：拥有“写入”及“读取及执行”权限的所有权限，还可删除文件夹。
- (6) 完全控制：拥有所有 NTFS 文件夹的权限，以及“更改”与“取得所有权”的权限。

提示



无论用何种权限保护文件，被允许对文件夹进行“完全控制”的组或用户都可以删除该文件夹内的任何文件。尽管“列出文件夹内容”和“读取及执行”看起来有相同的特殊权限，但是这些权限在继承时却有所不同。“列出文件夹内容”可以被文件夹继承，而不能被文件继承，并且只在查看文件夹权限时才会显示；“读取及执行”可以被文件和文件夹继承，并且在查看文件和文件夹权限时始终会出现。另外在 Windows Server 2008 家族中，默认情况下，Everyone 不包含 Anonymous（匿名），因此应用于 Everyone 的权限不影响 Anonymous。

2. 多重 NTFS 权限

可以为每个单独的用户账户及其所属的组指定权限，从而为一个用户账户指定多个用户权限。不过应先理解与如何指定 NTFS 权限和组合多个权限相关的规则和优先级，并了解 NTFS 权限的继承性。

(1) 权限是累积的

用户拥有的一个资源的最终权限是为该用户指定的全部 NTFS 权限及为该用户所属组指定的全部 NTFS 权限的和。如果一个用户有一个文件夹的读权限，同时又是对该文件夹有写入权限的用户组的成员，则该用户对这个文件夹既有读权限，也有写入权限。

例如，用户 Lxh 分属 Sales 和 Manager 组，其中 Sales 组对 Folder 文件夹拥有写入权限，Manager 对 Folder 文件夹拥有读取权限，那么 Lxh 则对 Folder 文件夹拥有读取和写入权限，如图 10-22 所示。

(2) 文件权限优先于文件夹权限

NTFS 文件权限优先于 NTFS 文件夹权限，用户只要拥有访问一个文件的权限，即使没有访问该文件所在文件夹的权限，仍然可以访问该文件。用户可以通过通用命令规则（UNC）或本地路径，从各自的应用程序打开有权访问的文件。即使该用户由于没有包含该文件夹的权限，而看不到该文件夹，但仍然可以访问那些文件。即如果没有访问包含打算访问文件所在的文件夹的权限，则必须要知道该

文件的完整路径才能访问它。没有访问该文件夹的权限，则不能看到该文件夹，也不能通过网上邻居等方式浏览访问。

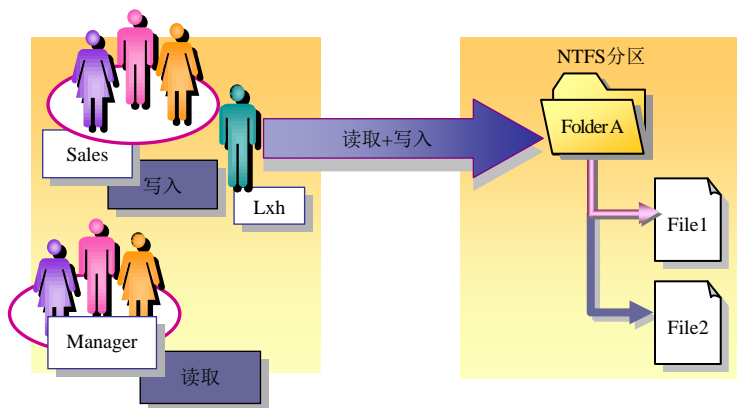


图 10-22 权限是累积的

例如，尽管 File2 属于 Folder 文件夹，并且 Sales 组对 Folder 文件夹拥有写入权限。但是如果 Sales 组只对 File2 拥有读取权限，那么用户 Lxh 也将只拥有对 File2 的读取权限，如图 10-23 所示。

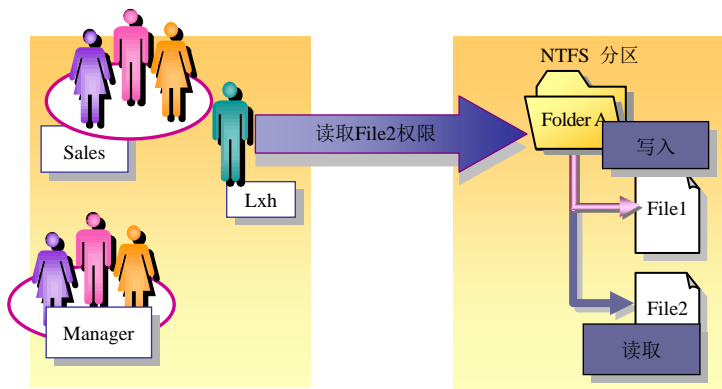


图 10-23 文件权限优先于文件夹权限

(3) 拒绝权限优先于其他权限

拒绝权限是指拒绝某个用户账户或用户组访问某个特定文件的权限，该权限优先于所有的允许权限。即使用户作为一个用户组的成员有权访问文件或文件夹，但是一旦为该用户设定了拒绝权限，则剥夺了其可能拥有的任何其他权限。应当尽量避免使用拒绝权限，因为允许用户和组进行某种访问比明确拒绝进行某种访问更容易做到。事实上，只需巧妙地构造组和组织文件夹中的资源，即可通过各种各样的“允许”权限满足访问控制的需要。

例如，用户 Lxh 同时属于 Sales 组和 Manager 组。其中 Lxh 拥有对 Folder A 的读取权限，Sales 拥有对 Folder A 的读取和写入权限，Manager 则被禁止对 File2 的写操作。因此 Lxh 拥有对 Folder A 和 File1 的读取和写入权限，但对 File2 只有读取权限，如图 10-24 所示。

3. NTFS 权限的继承性

默认情况下，为父文件夹指定的权限会由其所包含的文件夹和文件继承并传播给它们，当然也可以根据需要限制这种权限继承。

(1) 权限继承

文件和子文件夹从其父文件夹继承权限，为父文件夹指定的任何权限也适用于在该父文件夹中所包含的子文件夹和文件。当为一个 NTFS 文件夹指定权限时，不仅为该文件夹及其中所包含的文件和

子文件夹指定了权限，同时也为在该文件夹中创建的所有新文件和文件夹指定了权限。默认状态下，所有文件夹和文件都从其父文件夹继承权限。

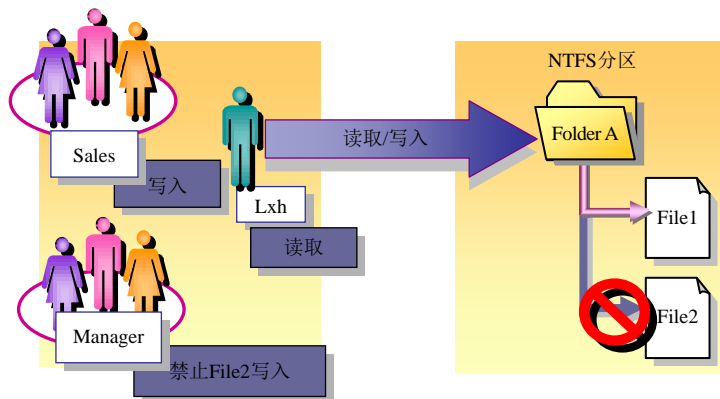


图 10-24 拒绝权限优先

例如，当允许权限继承时，为 Folder 设置的访问权限将自动被传递给 File1、SubF 和 File2。即子文件夹 SubF 和文件 File1、File2 将自动取得为父文件夹 Folder 设置的访问权限，如图 10-25 所示。

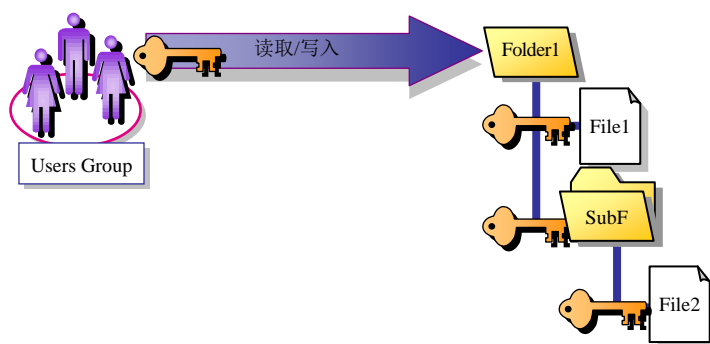


图 10-25 权限继承

(2) 禁止权限继承

可以禁止指定给一个父文件夹的权限被这个文件夹中所包含的子文件夹和文件继承，即子文件夹和文件不会继承指定给包含其父文件夹的权限。被禁止继承权限的文件夹变成新的父文件夹，为该文件夹指定的权限将会被其所包含的任何子文件夹和文件继承。

例如，当禁止权限继承时，为 Folder 设置的访问权限将不被传递给 File1、SubF 和 File2，如图 10-26 所示。即子文件夹 SubF 和文件 File1、File2 不能自动取得为父文件夹 Folder 设置的访问权限，必须一一为它们分别设置访问权限。

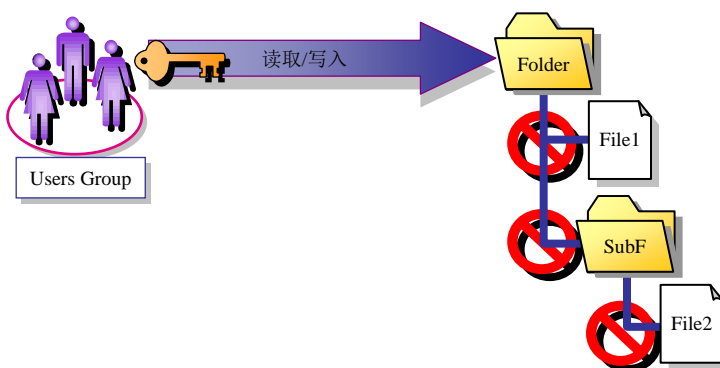


图 10-26 禁止权限继承

4. 共享文件夹权限与 NTFS 文件系统权限的组合

为快速有效地控制对 NTFS 磁盘分区中网络资源的访问，应利用默认的共享文件夹权限共享文件夹，然后通过授予 NTFS 权限控制对这些文件夹的访问。当共享的文件夹位于一个利用 NTFS 格式化的磁盘分区中时，该共享文件夹的权限即与 NTFS 权限相组合，用于保护文件资源。共享文件夹为资源提供有限的安全性，而 NTFS 权限为共享文件夹提供最大的灵活性。不论是在本地，还是通过网络访问该资源，NTFS 权限都起作用。因此除了设置 NTFS 权限外，还需要设置共享文件夹权限。

如果要为共享文件夹设置 NTFS 权限，可在共享文件夹的属性对话框中打开“安全”选项卡，设置其共享文件夹的 NTFS 权限。

共享文件夹权限具有以下特点。

(1) 共享文件夹权限只适用于文件夹，而不适用于单独的文件。并且只能为整个共享文件夹设置共享权限，而不能设置该共享文件夹中的文件或子文件夹，所以共享文件夹权限不如 NTFS 文件系统权限详细。

(2) 共享文件夹权限并不对直接登录到计算机上的用户起作用，它们只适用于通过网络连接该文件夹的用户，即共享权限对直接登录到服务器上的用户是无效的。

(3) 在 FAT/FAT32 系统卷上，共享文件夹权限是保证网络资源被安全访问的唯一方法。原因很简单，NTFS 权限不适用于 FAT/FAT32 卷。

(4) 默认的共享文件夹权限是读取，并被指定给 Everyone 组。

共享权限分为读取、修改和完全控制，不同权限及其对用户访问能力的控制如表 10-1 所示。

表 10-1 共享文件夹的权限及其对用户访问能力的控制

权 限	允许用户执行的操作
读取	显示文件夹名称、文件名称、文件数据和属性、运行应用程序文件，并改变共享文件夹内的文件夹
修改	创建文件夹、在文件夹中添加文件、修改文件内容、在文件中追加数据、修改文件属性、删除文件夹和文件，以及执行“读取”权限所允许的操作
完全控制	修改文件权限，获得文件的所有权 执行“修改”和“读取”权限所允许的所有操作，默认情况下，Everyone 组具有该权限

网络管理员组合 NTFS 权限和共享文件夹的权限时，组合结果所产生的权限或者是组合的 NTFS 权限，或者是组合的共享文件夹权限，哪个范围更窄是哪一个。

当在 NTFS 卷中为共享文件夹授予权限时，应当遵守下述规则。

(1) 可以为共享文件夹中的文件和子文件夹应用 NTFS 权限，并为共享文件夹中包含的每个文件和子文件夹应用不同的 NTFS 权限。

(2) 除共享文件夹权限外，用户必须要有该共享文件夹包含的文件和子文件夹的 NTFS 权限，才能访问这些文件和子文件夹。在 FAT 卷中共享文件夹权限是保护该共享文件夹中的文件和子文件夹的唯一权限。

(3) 在 NTFS 卷上必须要求 NTFS 权限，默认情况下，Everyone 组具有“完全控制”权限。

5. 文件与文件夹的所有权

在 NTFS 分区中每个文件与文件夹都有其“所有者”，系统默认是创建文件或文件夹的用户，即该文件或文件夹的所有者。所有者具有更改该文件夹或文件权限的能力。

Windows Server 2008 允许用户取得文件或文件夹的所有权，以更改其所有者。用户必须具备以下的条件之一，才可取得所有权。

(1) 拥有该文件或文件夹“取得所有权”的特殊权限。

(2) 系统管理员，即属于 Administrators 组的用户。无论其拥有文件或文件夹的哪种权限，永远都具有“取得所有权”的权限。

(3) 具备“取得文件或其他对象的所有权”权限的用户。

任何用户在变成文件或文件夹的所有者后，就可以更改该文件或文件夹权限，但是并不会影响自己的其他权限。同时文件夹或文件的所有权被夺取后，也不会影响原所有者的其他已有权限。

当用户要查看或夺取文件的所有权时，可在登录后右击文件，选择快捷菜单中的“属性”选项。在“安全”选项卡中单击“高级”按钮打开该文件的高级安全设置对话框，打开“所有者”选项卡，如图 10-27 所示。



图 10-27 “所有者”选项卡

单击“编辑”按钮，打开如图 10-28 所示的修改所有者对话框，在下边的列表框中选择要修改为所有者的用户名。如果其中没有要修改为其所有者的用户名，则单击“其他用户或组”按钮，将要修改为所有者的用户添加到列表中。



图 10-28 所有者对话框

修改完成后，单击“确定”按钮保存修改。需要注意的是，如果是刚刚获得此对象的所有权，在查看或更改权限之前，需要关闭并重新打开其属性。

如果用户属于 Administrators 组，则在更改文件或文件夹的所有权时，可以选择将所有权转移给自己、Administrators 组或者其他用户或组。

6. 复制或移动文件后的权限变化

对于 NTFS 分区内的文件，当复制或移动到另一个文件夹后，其权限可能会发生如下变化。

(1) 文件从某个文件夹复制到另一个文件夹时，无论文件被复制到同一个磁盘或不同的 NTFS 磁

盘内都等于产生了另一个新的文件，因此新文件的权限继承目的文件夹的权限。

(2) 文件从某文件夹移动到另一个文件夹时，如果移动到同一磁盘的另一个文件夹内，仍然会保持原来的权限；如果移动到另一个 NTFS 磁盘内，则该文件会继承目的地的权限。

将文件移动或复制到目的地的用户会成为该文件的所有者，文件夹的移动或复制的原理与文件相同。不过，如果将文件从 NTFS 磁盘移动或复制到 FAT 或 FAT32 磁盘内，则其原有的权限设置都将被删除，因为 FAT 或 FAT32 不支持 NTFS 权限设置的功能。

在移动文件或文件夹时，无论是移动到相同还是不同的 NTFS 磁盘，必须对源文件或文件夹具有“修改”的权限，并且必须对目的文件夹具有“写入”权限。

10.1.3 设置 NTFS 权限

在 NTFS 磁盘中，系统会自动设置默认的权限值，并且这些权限会被其子文件夹和文件所继承。为了控制用户对某个文件夹以及该文件夹中的文件和子文件的访问，需要指定文件夹权限。设置文件或文件夹的权限必须是 Administrators 组的成员、文件/文件夹的所有者，以及具备完全控制权限的用户。

1. NTFS 文件夹权限

打开 Windows 资源管理器，右击待设置 NTFS 权限的文件夹，如 tools。在快捷菜单中选择“属性”选项，打开“tools 属性”对话框。打开“安全”选项卡，如图 10-29 所示。默认已经有一些权限设置，这些设置是从父文件夹（或磁盘）所继承的。例如，在“User”组的权限列表中，灰色阴影对勾的权限就是继承来的。

如要更改权限，则单击“编辑”按钮，打开如图 10-30 所示“tools 的权限”对话框。在“组或用户名”列表框中选中待设置权限的用户名，在下方的权限下拉列表框中选中“允许”或“拒绝”复选框。虽然更改从父项对象所继承的权限，例如添加其权限，或者通过选中“拒绝”复选框删除权限，但是不能够直接将灰色的对勾删除。



图 10-29 “安全”选项卡



图 10-30 “安全”选项卡

如果为其他用户指定权限，则单击“添加”按钮，从本地计算机中添加拥有对该文件夹访问和控制权限的用户或用户组。如图 10-31 所示，用户组中的用户将拥有和用户组同样的权限，可在“输入对象名称来选择”文本框中键入用户名。如果不知道用户名，则单击“高级”按钮，并单击“立即查找”按钮查找已经存在的用户。

单击“确定”按钮，添加到“组或用户名”列表框中，如图 10-32 所示。由于新添加用户的权

限不是从父项继承的，因此新用户所有的权限都可以修改。



图 10-31 添加用户或用户组



图 10-32 修改用户权限

如果不想继承上一层的权限，可在“安全”选项卡中单击“高级”按钮，显示如图 10-33 所示的“tools 的高级安全设置”对话框。



图 10-33 “tools 的高级安全设置”对话框

单击“编辑”按钮，打开如图 10-34 所示的“tools 的高级安全设置”对话框。在“权限项目”下拉列表框中选待修改的用户，然后单击“编辑”按钮修改其相应的权限。



图 10-34 “tools 的高级安全设置”对话框

清除“包括可从该对象的父项继承的权限”复选框，显示如图 10-35 所示的“Windows 安全”对话框。单击“复制”按钮保留原来从父项对象继承的权限，单击“删除”按钮将此权限删除。

2. NTFS 文件权限

文件权限的设置与文件夹相似，要为文件指定 NTFS 权限，可打开 Windows 资源管理器。右击文件名，如“help.txt”，选择快捷菜单中的“属性”选项。显示“help.txt 属性”对话框，打开“安全”选项卡，在其中为其设置权限，如图 10-36 所示。

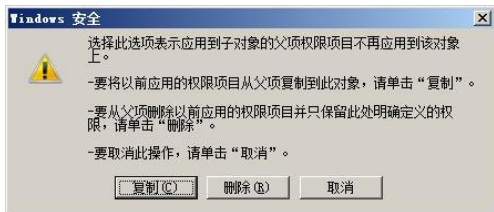


图 10-35 “Windows 安全”对话框

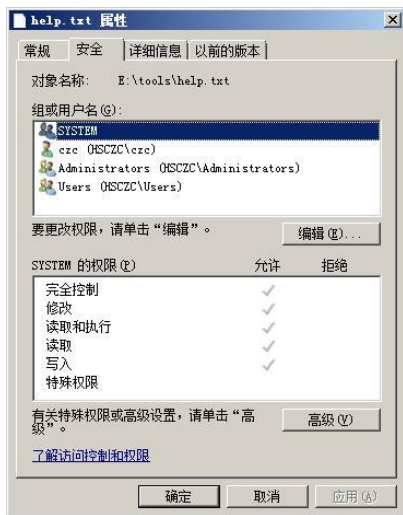


图 10-36 设置文件权限

3. 特殊访问权限

标准 NTFS 权限通常可满足一般的需求，如果用户要更精确地指定权限，以满足各种不同的权限需求，则需要借助于特殊访问权限。

以 tools 文件为例，打开其属性对话框中的“安全”选项卡。单击“高级”按钮，显示如图 10-37 所示的“tools 高级安全设置”对话框。



图 10-37 “tools 高级安全设置”对话框

单击“编辑”按钮，显示如图 10-38 所示的“tools 权限项目”对话框，在其中可以更精确地设置用户的权限。

特殊访问权限共有 13 项，组合在一起构成了标准的 NTFS 权限。例如，标准的“读取”权限包含“读取数据”、“读取属性”、“读取权限”和“读取扩展属性”4 种特殊访问权限。有两个特殊访问权限

对于管理文件和文件夹的访问来说特别有用，一是更改权限；二是获得所有权。

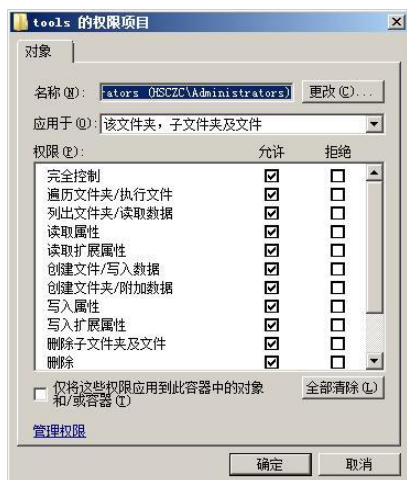


图 10-38 “tools 权限项目”对话框

(1) 更改权限：为某用户授予该权限，该用户则具有了针对文件或者文件夹修改权限的功能。借助于更改权限，可以将修改文件或文件夹的权限授予其他管理员和用户，但是不授予其对该文件或文件夹的“完全控制”权限。通过这种方式，这些管理员或者用户不能删除或者写入该文件或文件夹，但是可以为该文件或文件夹授权。为了将修改权限的能力授予网络管理员，将针对该文件或文件夹的“更改权限”权限授予 Administrators 组即可。

(2) 获得所有权：为用户授予这一权限，该用户就具有了取得文件和文件夹的所有权。借助于该权限，可以将文件和文件夹的拥有权从一个用户账户或者组转移到另一个用户账号或者组。也可以将“获得所有权”这种权限授予某个用户，网络管理员也可以获得某个文件或文件夹的所有权。

在获得某个文件或者文件夹的所有权时，应当遵循以下规则。

(1) 当前拥有者或者具有“完全控制”权限的任何用户可以将“完全控制”这一标准权限或者“获得所有权”这一特殊访问权限授予另一个用户账户或者组，这样该用户账户或者该组的成员可获得所有权。

(2) Administrators 组的成员可以取得某个文件或者文件夹的所有权，而忽略该文件夹或者文件授予的权限。如果某个管理员取得了所有权，则 Administrators 组也取得了所有权。因而该管理员组的任何成员都可以修改针对该文件或者文件夹的权限，并且可以将“获得所有权”这一权限授予另一个用户账户或者组。

例如，如果某个雇员离开了原来的公司，某个管理员即可取得该雇员的文件的所有权。并将“取得所有权”这一权限授予另一个雇员，然后这一雇员就取得了前一雇员的文件的所有权。

为了成为某个文件或者文件夹的拥有者，具有“获得所有权”这一权限的某个用户或者组的成员必须明确地取得该文件或者文件夹的所有权，而不能自动将某个文件或者文件夹的所有权授予任何一个人。文件的拥有者、管理员组的成员或者任何一个具有“完全控制”权限的用户都可以将“获得所有权”权限授予某个用户账户或者组，这样就使其获得了所有权。

10.1.4 访问共享文件夹

设置资源共享以后，用户可以采用多种方式实现访问文件服务器，并使用文件服务器中的共享资源。下面以客户端系统使用 Windows Vista 为例介绍。

1. 网上邻居

网络上所有的共享文件夹都会显示在“网上邻居”中，如果用户拥有相应的访问权限，则可访问

该共享文件。

① 单击“开始”→“网络”选项，打开“网络”窗口，如图 10-39 所示。系统会自动搜索网络中的计算机，并将计算机名显示在该窗口中。

② 选择要访问的计算机名，双击即可打开。如果需要登录才能访问，则会显示如图 10-40 所示“连接到...”对话框。键入具有访问共享权限的用户名和密码。

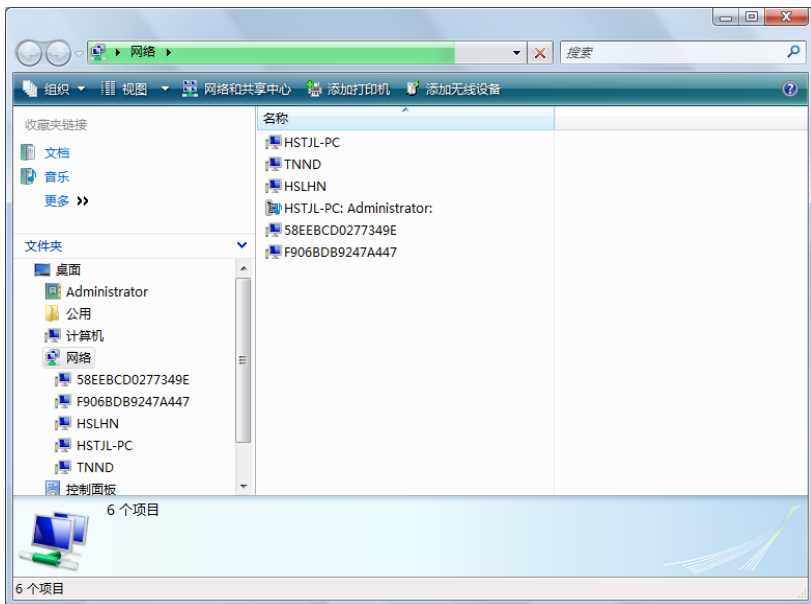


图 10-39 “网络”窗口

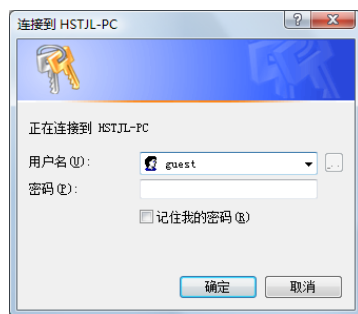


图 10-40 “连接到...”对话框

③ 单击“确定”按钮，显示该计算机中的共享文件夹，如图 10-41 所示。

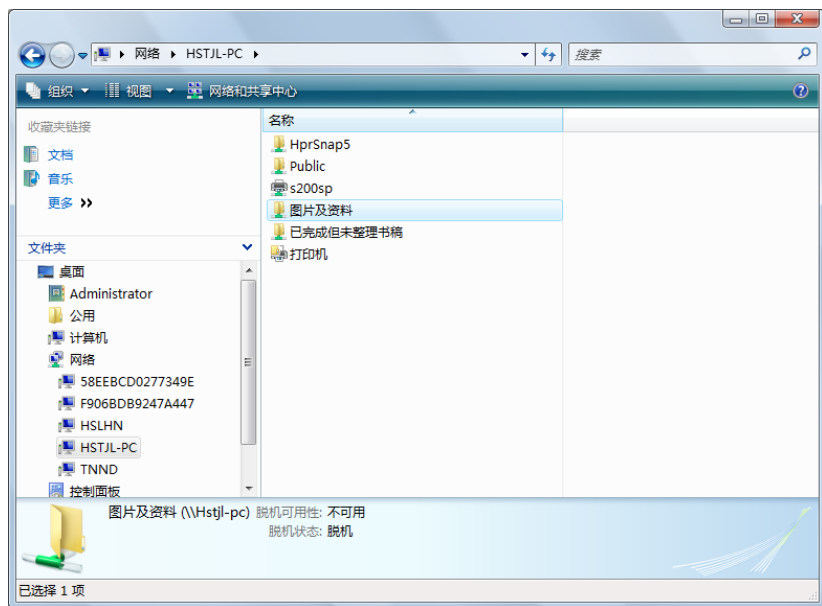


图 10-41 共享文件夹

④ 双击打开要访问的共享文件夹，显示其中的文件，如图 10-42 所示。此时可以复制该共享文件夹中的文件，或者在其中写入文件。

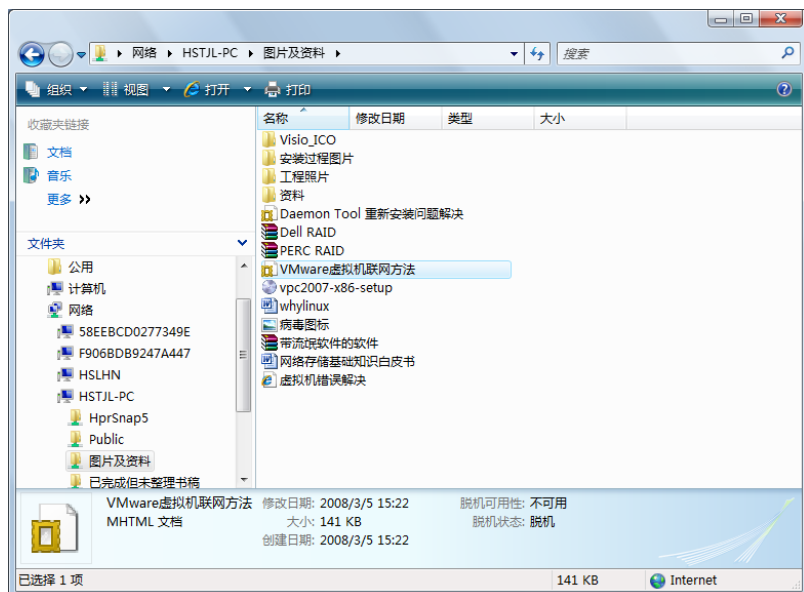


图 10-42 共享文件夹中的文件

注意：

打开“网上邻居”窗口所需要的时间较长，并且共享文件夹的更新速度较慢。另外，如果用户为非正常关机，那么尽管在“网上邻居”窗口中显示该计算机，但是却无法通信。



2. 搜索共享文件

如果已经知道计算机的 IP 地址或计算机名，那么还可以利用 Windows Vista 的搜索功能搜索所需要的某个文件。

- ① 单击“开始”→“搜索”选项，显示如图 10-43 所示的“搜索结果”窗口。



图 10-43 “搜索结果”窗口

- ② 单击“高级搜索”按钮，显示如图 10-44 所示的搜索设置的窗口，在其中设置详细的搜索信息。



图 10-44 搜索设置窗口

③ 在“位置”下拉列表框中选择“选择搜索位置”选项，显示如图 10-45 所示的“选择搜索位置”对话框。在“添加”文本框中键入要搜索的计算机名，格式为：\\计算机名。

④ 单击“添加”按钮，添加到“所选位置的摘要”列表框中。其中列出该计算机中的所有共享文件夹，用户可以选择要搜索的共享文件夹。默认选中所有共享文件，如图 10-46 所示。

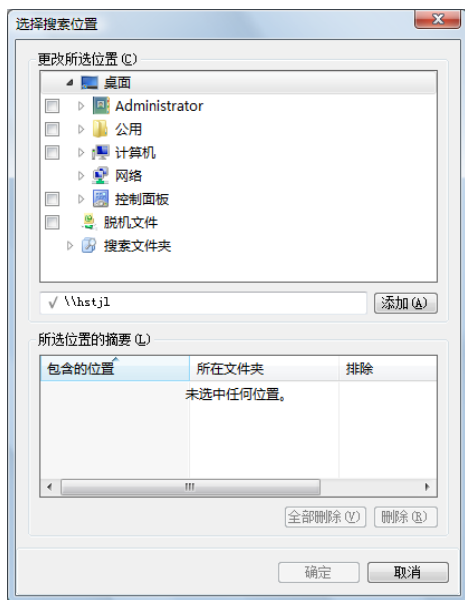


图 10-45 “选择搜索位置”对话框

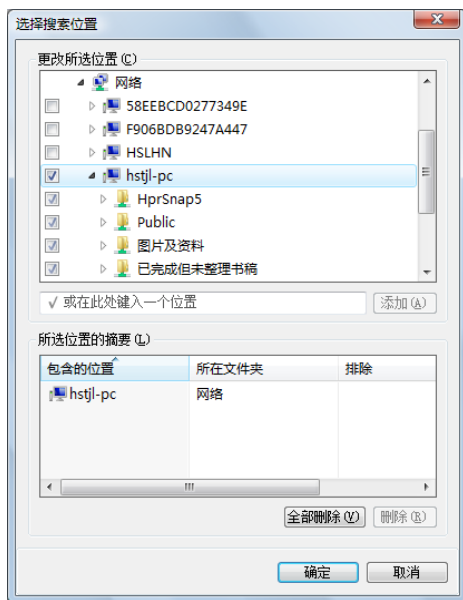


图 10-46 所有共享文件

⑤ 单击“确定”按钮返回“搜索结果”窗口，在“名称”文本框中键入要搜索的文件或文件夹名。单击“搜索”按钮，显示该计算机上所有符合条件的内容，如图 10-47 所示。此时，可以直接打开所需要的共享文件。

3. 映射网络驱动器

如果需要经常访问文件服务器中的共享资源，显然每次借助“网上邻居”或者“搜索计算机”的方式非常麻烦。此时可以采用映射网络驱动器的方式，将共享文件夹映射为本地计算机的一个网络驱动器，这样以后不需输入共享地址即可如访问本地硬盘一样访问。

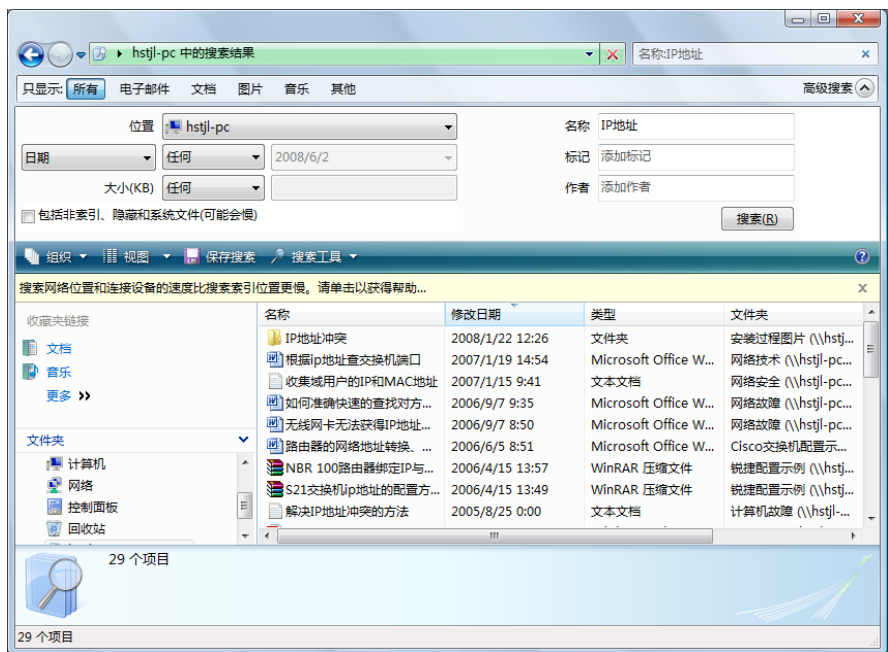


图 10-47 共享文件搜索结果

① 打开“开始”菜单，右击“计算机”选项。选择快捷菜单中的“映射网络驱动器”选项，显示如图 10-48 所示的“映射网络驱动器”对话框。在“驱动器”下拉列表框中选择一个驱动器盘符，在“文件夹”文本框中键入共享文件夹的地址，格式为“\\计算机名或 IP 地址\共享文件夹名”。

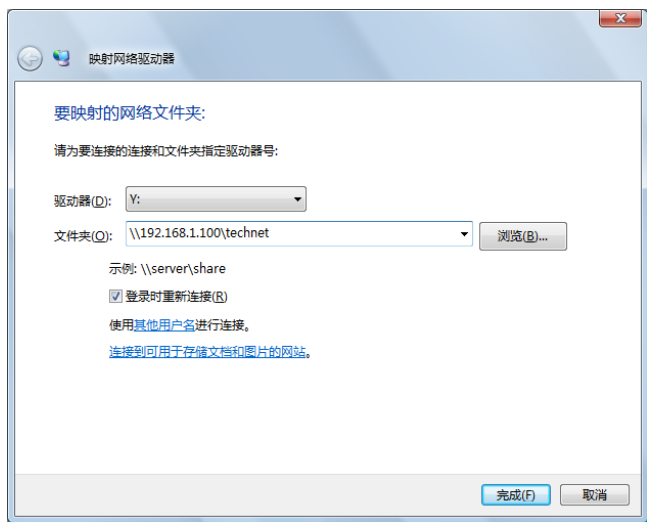


图 10-48 “映射网络驱动器”对话框

② 单击“完成”按钮，将该共享文件夹映射为网络驱动器，如图 10-49 所示，以后即可如访问本地磁盘一样访问共享文件。

4. Windows 资源管理器

如果已经知道共享文件夹所在计算机的计算机名或 IP 地址，则可在 Windows 资源管理器的地址栏中直接输入地址，格式为：

\\计算机名或 IP 地址\共享文件夹名

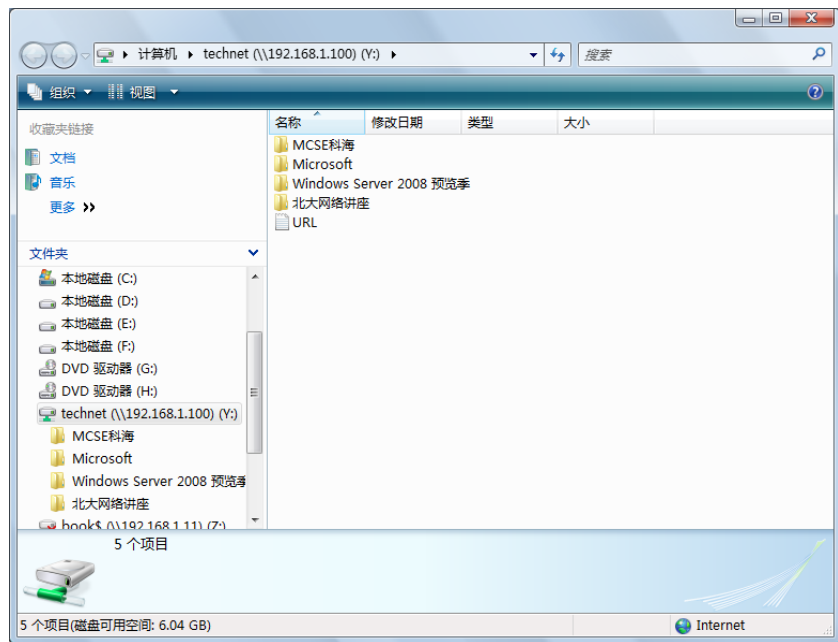


图 10-49 网络驱动器

例如，输入\\192.168.1.100。按回车键，显示文件服务器中的共享资源，当然用户必须拥有相应的访问权限才行。

10.2 安装文件服务器

安装文件服务器的操作步骤如下。

① 打开“服务器管理器”窗口，运行“添加角色向导”，在如图 10-50 所示的“选择服务器角色”对话框中选中“文件服务”复选框。

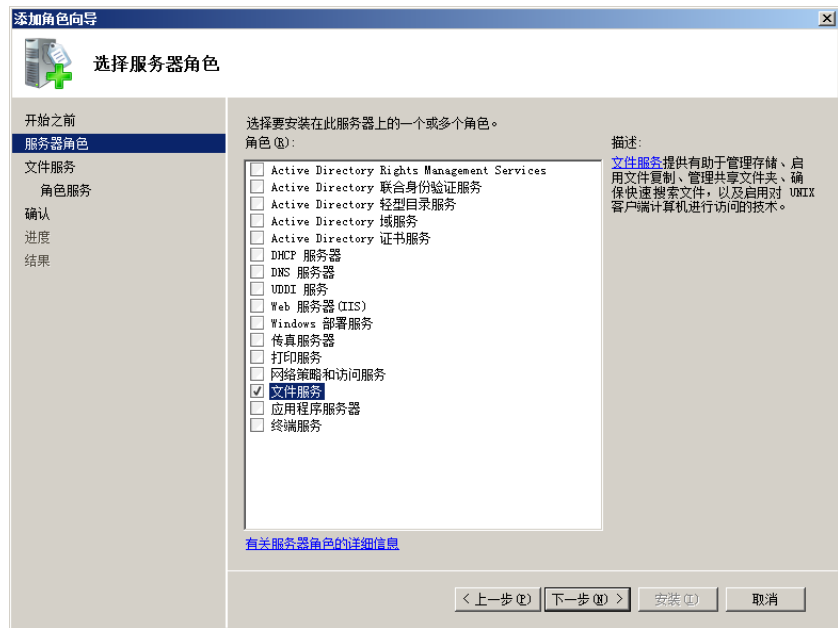


图 10-50 “选择服务器角色”对话框

② 单击“下一步”按钮，显示如图 10-51 所示的“文件服务”对话框。其中列出文件服务简介，

以及一些相关的注意事项等。



图 10-51 “文件服务”对话框

③ 单击“下一步”按钮，显示如图 10-52 所示的“选择角色服务”对话框，选择所要安装的服务组件。文件服务的组件包括文件服务器、分布式文件系统、文件服务器资源管理器、网络文件系统服务、Windows 搜索服务和 Windows Server 2003 文件服务。

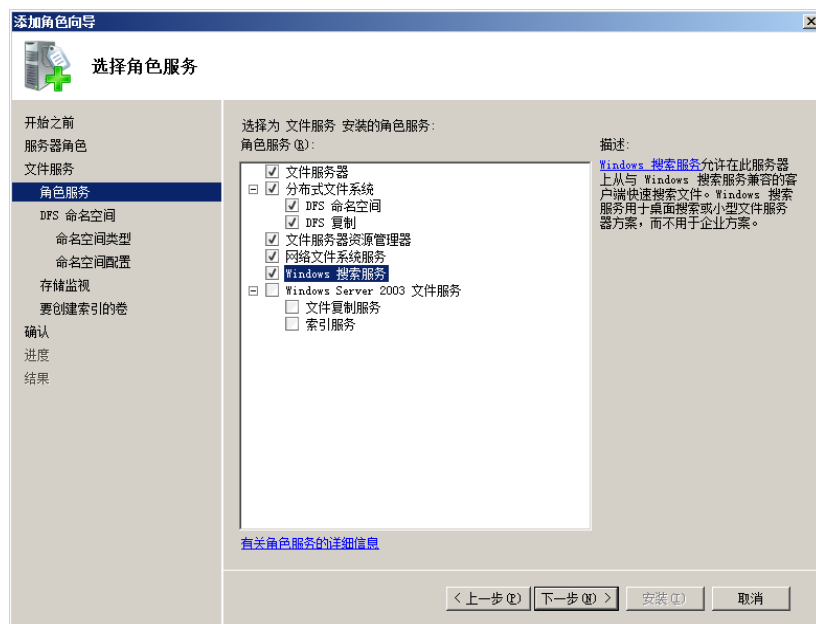


图 10-52 “选择角色服务”对话框

④ 单击“下一步”按钮，显示如图 10-53 所示的“创建 DFS 命名空间”对话框。默认选择“立即使用此向导创建命名空间”单选按钮，可在“输入此命名空间的名称”文本框中设置一个新名称。

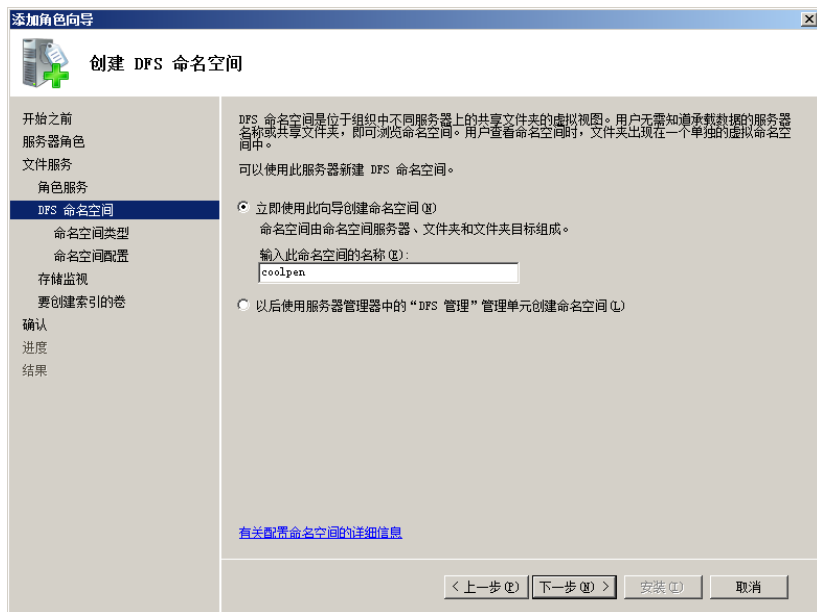


图 10-53 “创建 DFS 命名空间”对话框

⑤ 单击“下一步”按钮，显示如图 10-54 所示的“选择命名空间类型”对话框。由于当前基于域环境，因此选择“基于域的命名空间”单选按钮；如果是独立服务器，则选择“独立命名空间”单选按钮。

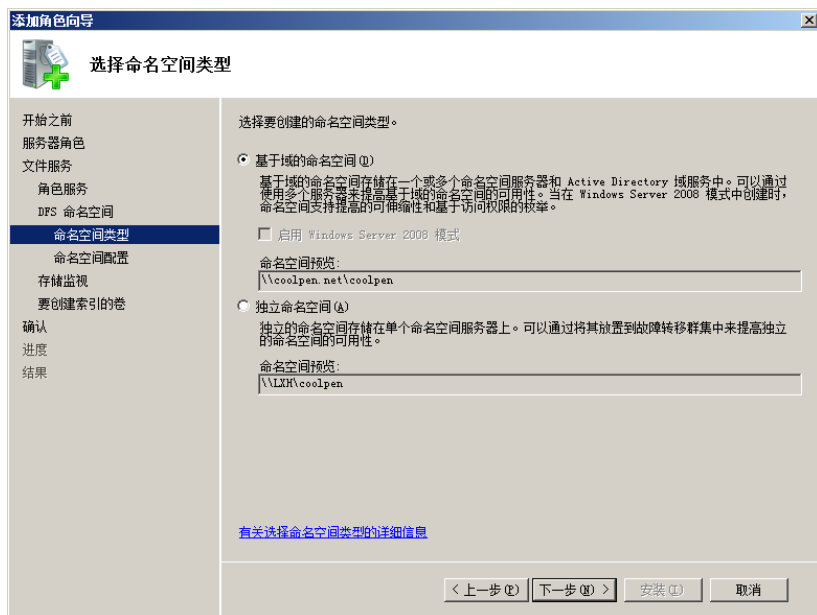


图 10-54 “选项命名空间类型”对话框

⑥ 单击“下一步”按钮，显示如图 10-55 所示的“配置命名空间”对话框，在“命名空间”列表框中显示前面所创建的命名空间。

⑦ 单击“下一步”按钮，显示如图 10-56 所示的“配置存储使用情况监视”对话框，其中显示本地计算机上的卷。网络管理员可以监控命名空间设置目录所在的磁盘空间，如果达到设置阈值，将启动报警功能。



图 10-55 “配置命名空间”对话框

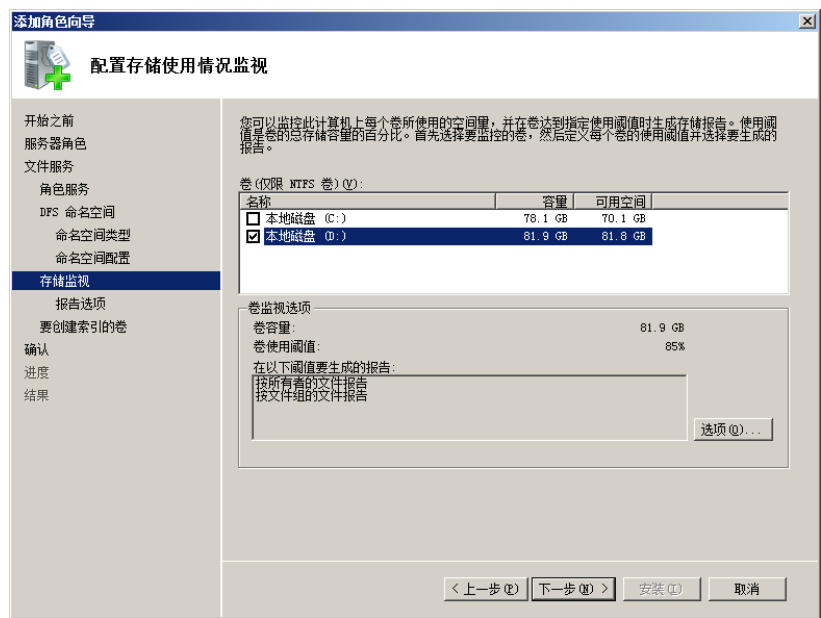


图 10-56 “配置存储使用情况监视”对话框

单击“选项”按钮，显示如图 10-57 所示的“卷监视选项”对话框，在“报告”列表框中可以选择要对卷的哪些使用情况生成报告。

⑧ 单击“下一步”按钮，显示如图 10-58 所示的“为 Windows 搜索服务选择要创建索引的卷”对话框。选择需要创建索引服务的卷，创建索引后客户端检索服务器中文件的速度将大幅度提升。不过，在创建索引的过程中，将消耗系统资源及空间。

⑨ 单击“下一步”按钮，显示如图 10-59 所示的“确认安装选择”对话框。其中列出前面所做的设置，如果需要更改，则单击“上一步”按钮返回。

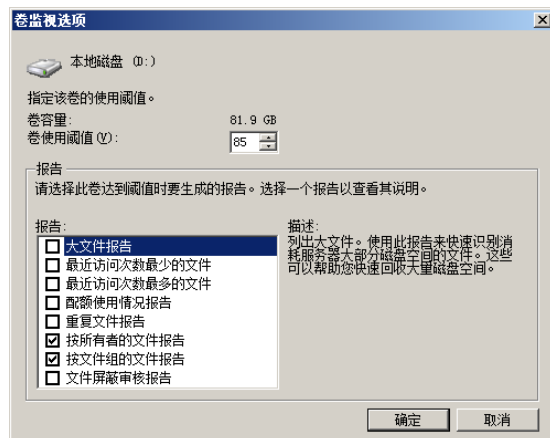


图 10-57 “卷监视选项”对话框

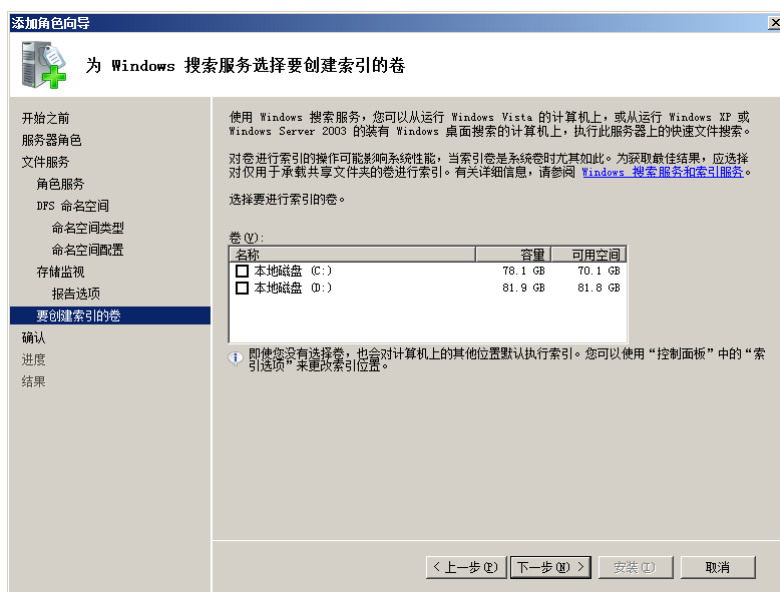


图 10-58 “为 Windows 搜索服务选择要创建索引的卷”对话框



图 10-59 “确认安装选择”对话框

⑩ 单击“安装”按钮，开始安装。完成后显示如图 10-60 所示的“安装结果”对话框，提示安装完成。



图 10-60 “安装结果”对话框

⑪ 单击“关闭”按钮，安装完成。重新打开“服务器管理器”窗口，在“文件服务”下即可看到已安装的组件，如图 10-61 所示。

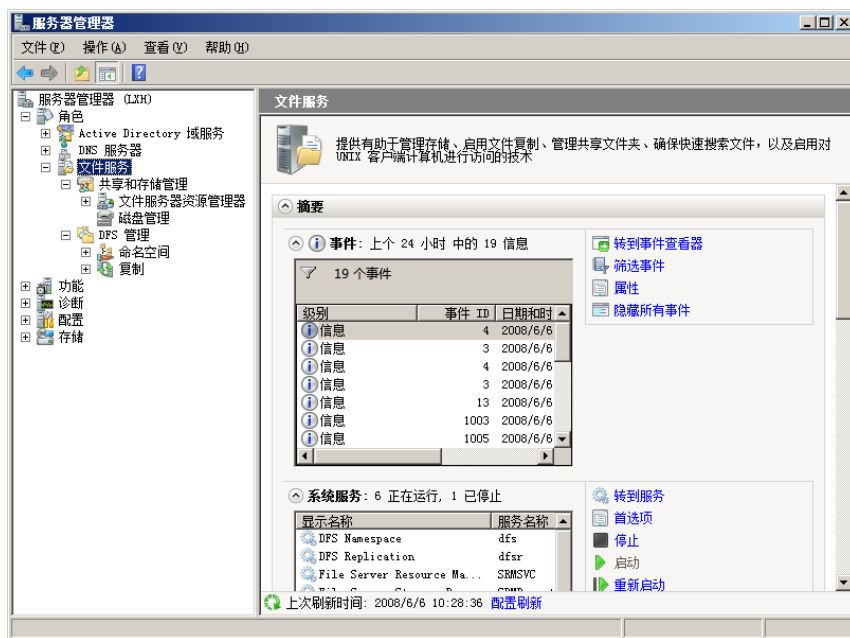


图 10-61 已安装的组件

10.3 分布式文件系统

如果局域网中有多台服务器，并且共享文件夹也分布在不同的服务器中，这样不利于系统管理员的管理和用户的访问。而使用分布式文件系统（Distributed File System，DFS），系统管理员就可以把不同服务器中的共享文件夹组织在一起构建成一个目录树。这样在用户看来，所有共享文件仅存储在

一个地点。只需访问一个共享的 DFS 根目录，即可访问分布在网络中的文件或文件夹，而不必知道这些文件的实际物理位置。

►► 10.3.1 特点及应用

借助于 DFS 可以为网络中的所有共享文件提供一个访问点和一个逻辑树结构，使分布在多台服务器中的文件如同位于网络上的一个位置一样显示在用户面前，而忽略这些共享资源在网络中的位置。而且还可以将一些文件同时放在多台服务器中，当用户读取文件时，DFS 会从不同的服务器为用户读取，从而减轻一台服务器的负担。而且即使有一台服务器发生故障，DFS 仍然可以从其他服务器正常读取。

1. DFS 的特性

DFS 可以让用户很容易地从一个地点访问所需的文件，其重要特性如下。

(1) 访问文件更加容易

即使所需访问的文件可能在物理上分布于多台服务器中，用户也只需转到网络上的一个位置访问。而且当更改目标的物理位置时，不会影响用户访问文件夹。因为文件的位置看起来相同，所以仍然可以使用与以前相同的方式访问文件夹，并且不再需要进行多个驱动器映射即可访问其中的文件。另外，文件服务器的维护、软件升级和其他任务（一般需要服务器脱机）也可以在不中断用户访问情况下完成。这对 Web 服务器特别有用，因为通过选择网站的根目录作为 DFS 根目录可以在分布式文件系统中移动资源，而不会断开任何 HTML 链接。

(2) 高可用性

DFS 以两种方法确保用户对其文件的访问，一是服务器自动将 DFS 映射发布到 Active Directory 中，从而确保 DFS 名称空间对于域中所有服务器上的用户总是可视的；二是系统管理员可复制 DFS 根目录和目标，即在域中的多台服务器中复制 DFS 根目录和目标。这样即使在保存这些文件的某台物理服务器不可用，用户仍然可以访问所需文件。

(3) 服务器负载平衡

DFS 根目录可以支持将文件分布在网络中的多台服务器上，这个特性很有用。例如，某个文件将被用户频繁访问。如果允许所有用户都从该服务器访问，势必会加重其负担。而 DFS 可确保用户对该文件的访问分布于多台服务器，可以分散地从不同的服务器中读取文件。而在用户看来，该文件是驻留在网络的同一个位置上。而且即使有一台服务器发生故障，DFS 仍然可以从其他服务器正常读取。

(4) 文件和文件夹更为安全

DFS 使用标准 NTFS 和文件共享权限管理共享资源，所以可使用以前的安全组和用户账户以确保只有授权的用户才能访问敏感数据。

2. DFS 的类型

分布式文件系统有两种类型，一是独立的根目录分布式文件系统；二是域分布式文件系统。

独立的根目录分布式文件系统的目录配置信息存储在本地主服务器上，访问根或链接的路径以主服务器名称开始。它只有一个根目标（如图 10-62 所示），没有根级别的容错。因此当根目标不可用时，整个 DFS 名称空间都不可访问。

独立的 DFS 根目录具有以下特点。

(1) 不使用 Active Directory。

(2) 至多只能有一个根目录级别的目标。

(3) FRS（File Replication Service，文件复制服务）不支持自动文件复制。

(4) 通过服务器群集支持容错。

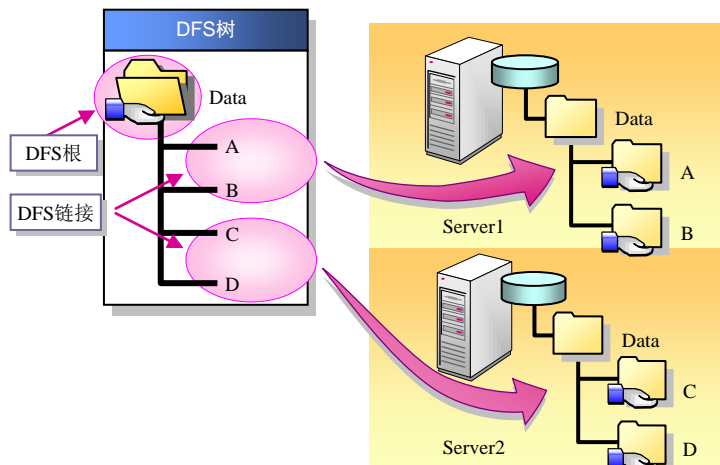


图 10-62 独立的分布式文件系统

在域分布式文件系统中，DFS 拓扑信息被存储在活动目录中。因为该信息对域中多个域控制器都可用，所以域 DFS 为域中的所有分布式文件系统提供容错。

域 DFS 根目录具有以下特点。

- (1) 必须宿主在域成员服务器上。
- (2) 其 DFS 名称空间自动发布到 Active Directory 中。
- (3) 可以有多个根目录级别的目标。
- (4) 通过 FRS 支持自动文件复制。
- (5) 通过 FRS 支持容错。

3. DFS 映射

DFS 映射由一个 DFS 根目录、一个或多个 DFS 链接，以及指向一个或多个目标的引用组成，如图 10-63 所示。

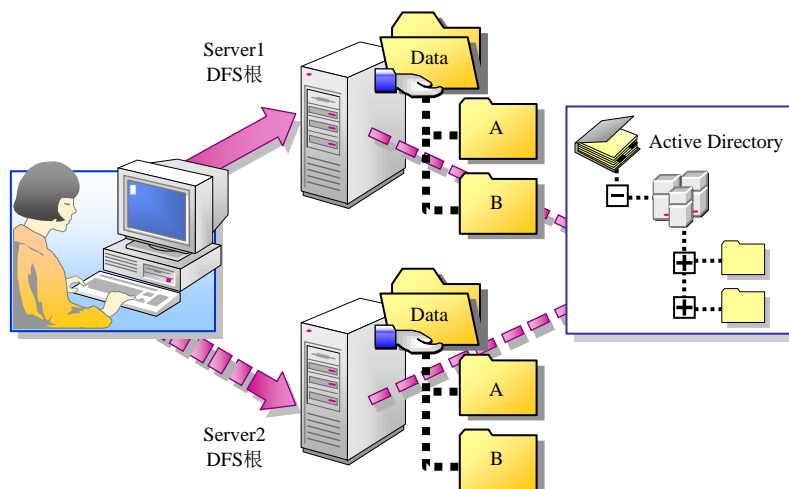


图 10-63 DFS 映射

DFS 根目录所驻留的域服务器称为“主服务器”。通过在域中的其他服务器上创建根目标可以复制 DFS 根目录。从而确保在主服务器不可用时，文件仍可使用。

DFS 映射为用户提供了对所需网络资源的统一和透明的访问，对于系统管理员来说，DFS 映射是

单独的 DNS 名称空间。通过域 DFS，DFS 根目标的 DNS 名称被解析到 DFS 根目录的主服务器。

由于域分布式文件系统的主服务器是域中的成员服务器，因此默认情况下 DFS 映射将自动发布到 Active Directory 中，从而提供了跨越主服务器的 DFS 拓扑同步。反过来又为 DFS 根目录提供了容错性，并支持目标的可选复制。

通过在 DFS 根目录中添加 DFS 链接可扩展 DFS 映射，Windows Server 2003 对 DFS 映射中分层结构层数的唯一限制是对任何文件路径最多使用 260 个字符。新 DFS 链接可以引用具有或没有子文件夹的目标，或引用整个 Windows Server 2003 家族卷。如果有适当的权限，也可以访问那些存在于或被添加到目标中的任何本地子文件夹。

客户端访问 DFS 的过程如图 10-64 所示。

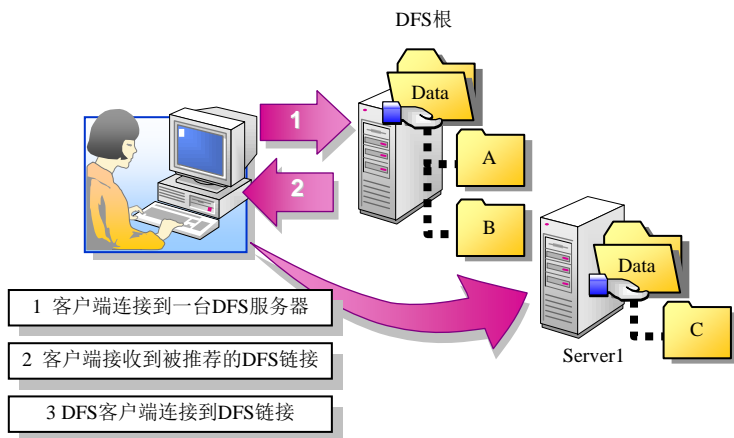


图 10-64 客户端访问 DFS 的过程

10.3.2 创建 DFS 映射

文件服务器在安装时可以创建命名空间，但是还需要网络管理员手动将网络中的共享文件夹添加到命名空间中，使用户在访问命名空间时即可访问网络中所有的共享文件夹。

提示



如果文件分布在多台服务器上，每台服务器的共享文件夹需要网络管理员在每台计算机上创建，或者使用其他远程控制台工具创建。创建连接并不能自动创建共享文件夹，共享文件夹需要手动提前创建，并且指定文件夹的访问权限。创建连接只是建立一个目标文件夹映射而已。

① 打开如图 10-65 所示的“服务器管理器”窗口，依次展开“角色”→“文件服务”→“DFS 管理”→“命名空间”→“\\coolpen.net\coolpen”选项。

② 右击命名空间“\\coolpe.net\coolpen”，从快捷菜单中选择“新建文件夹”选项。显示如图 10-66 所示的“新建文件夹”对话框，在“名称”文本框中键入新建文件夹的名称。

③ 单击“添加”按钮，显示如图 10-67 所示的“添加文件夹目标”对话框，添加网络中的共享文件夹。

④ 单击“浏览”按钮，显示“浏览共享文件夹”对话框。在“服务器”文本框中键入计算机名称，或者单击“浏览”按钮选择。然后单击“显示共享文件夹”按钮，显示该计算机中的共享文件夹，如图 10-68 所示。

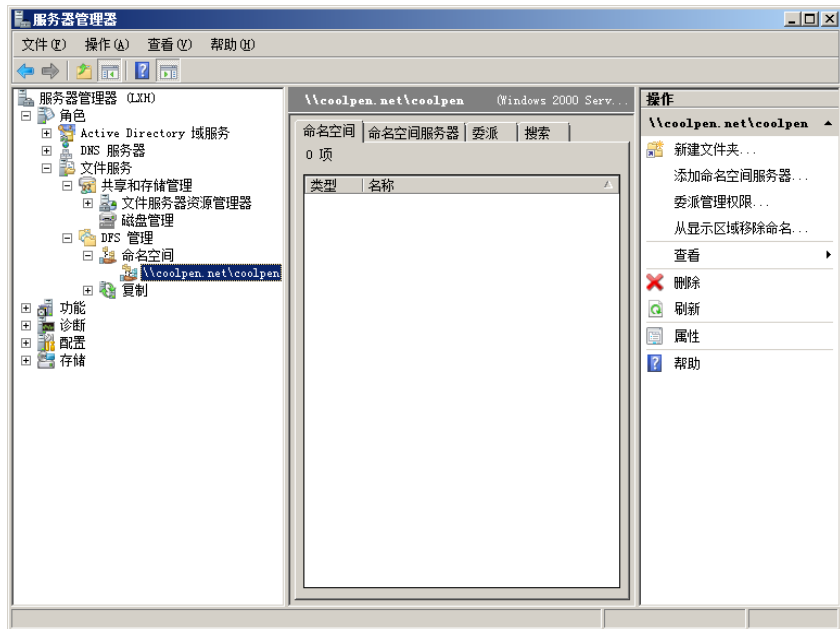


图 10-65 “服务器管理器”窗口

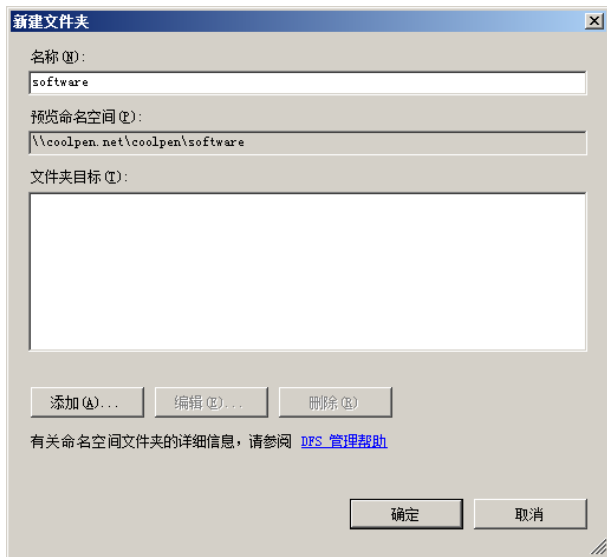


图 10-66 “新建文件夹”对话框

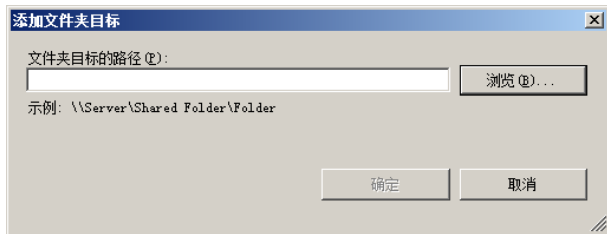


图 10-67 “添加文件夹目标”对话框

- ⑤ 单击“确定”按钮，在“共享文件夹”列表框中选择目标共享文件夹。单击“确定”按钮，关闭“浏览共享文件夹”对话框。返回到“添加文件夹目标”对话框，如图 10-69 所示。
- ⑥ 单击“确定”按钮，关闭“添加文件夹目标”对话框，返回到“新建文件夹”对话框，如图 10-70 所示。



图 10-68 “浏览共享文件夹”对话框

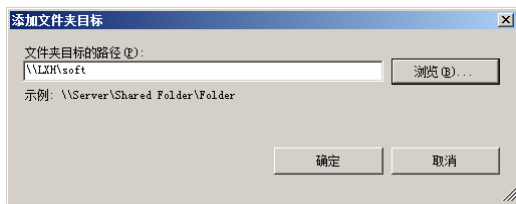


图 10-69 “添加文件夹目标”对话框

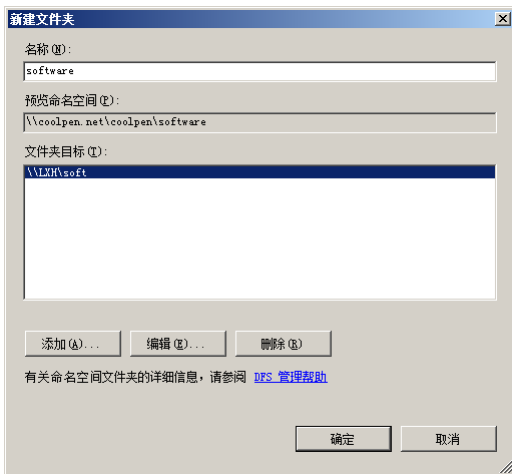


图 10-70 “新建文件夹”对话框

⑦ 单击“确定”按钮，创建完成新文件夹。

使用同样方法可以创建连接到其他成员服务器的共享文件夹，创建完成的 DFS 映射文件夹如图 10-71 所示。

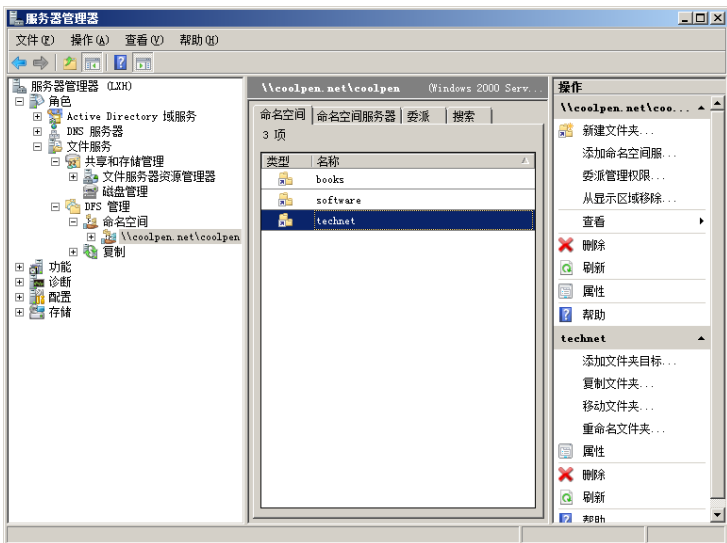


图 10-71 创建完成的 DFS 映射文件夹

10.3.3 DFS 复制

DFS 复制是一种文件存储功能，将分散在成员服务器的数据集中自动同步到中心服务器，网络管理员统一备份存储，成员服务器相当于中心服务器的一个子集。如果出现故障，可以继续使用中心服务器的数据，保证数据的安全。在默认情况下，汇聚方向为双向，网络管理员可以动态调整数据复制的方向。

① 在如图 10-72 所示的“服务器管理器”窗口中展开“角色”→“文件服务”→“DFS 管理”→“复制”选项。

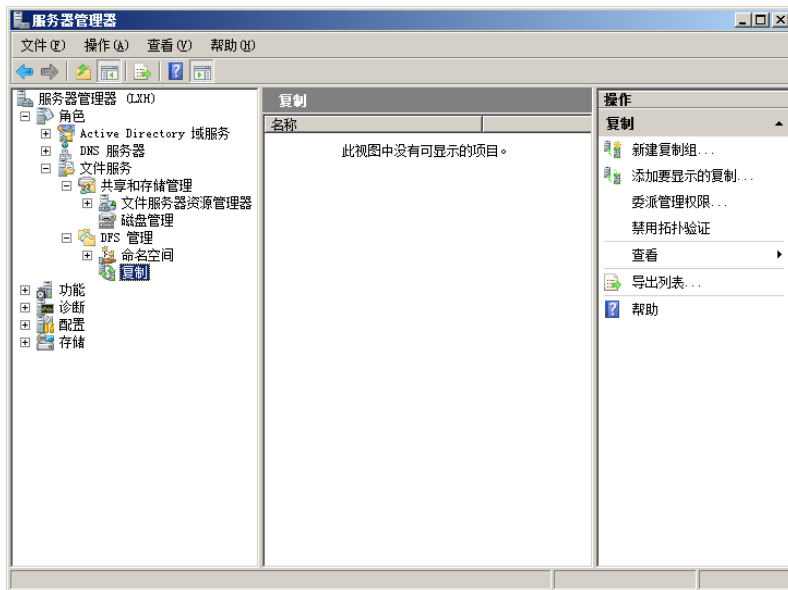


图 10-72 “服务器管理”窗口

② 右击“复制”并选择快捷菜单中的“新建复制组”选项，显示如图 10-73 所示的“复制组类型”对话框。选择“用于数据收集的复制组”单选按钮，以从成员服务器中收集数据。

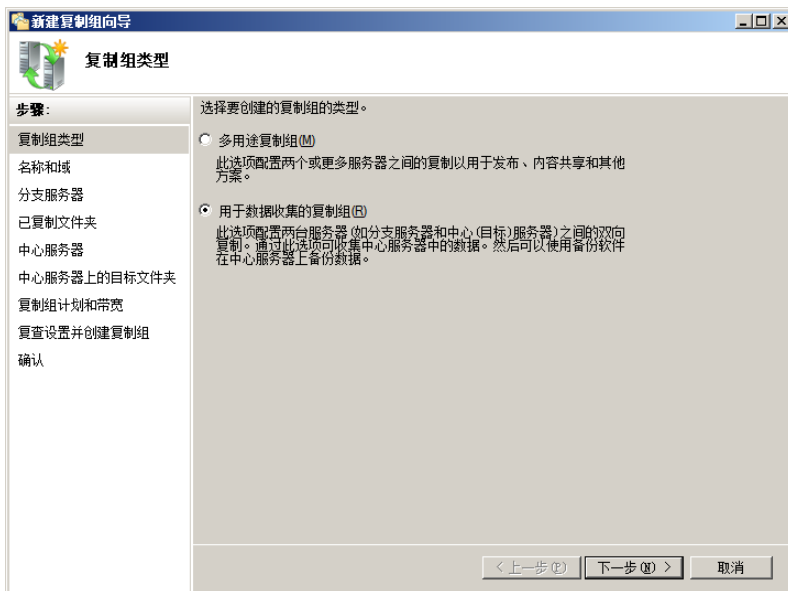


图 10-73 “复制组类型”对话框

③ 单击“下一步”按钮，显示如图 10-74 所示的“名称和域”对话框。键入复制组的名称，选择复制组的作用域，默认是当前服务器所在的 Active Directory。



图 10-74 “名称和域”对话框

④ 单击“下一步”按钮，显示如图 10-75 所示的“分支服务器”对话框。键入数据来源服务器名称，即数据要从哪台服务器收集，或者单击“浏览”按钮选择。

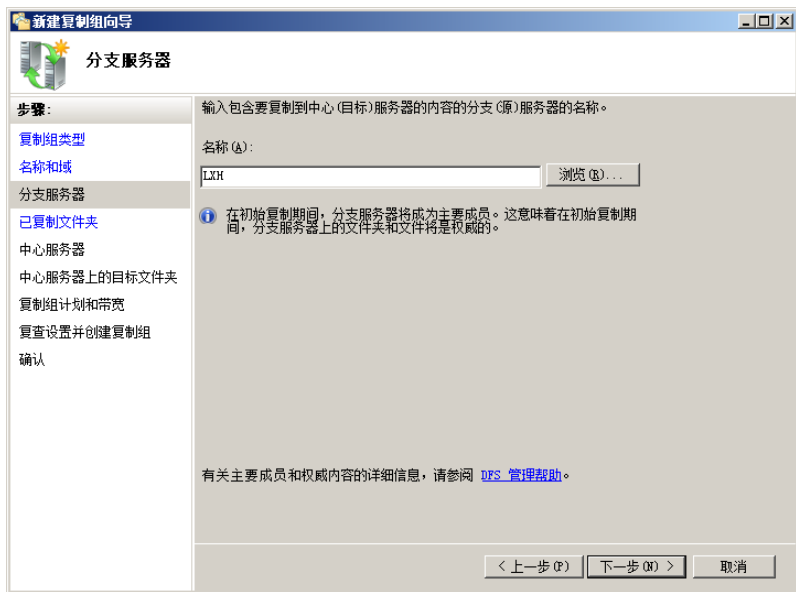


图 10-75 “分支服务器”对话框

提示 目标服务器中也必须安装 DFS 复制服务才能实现数据复制。

⑤ 单击“下一步”按钮，显示如图 10-76 所示的“已复制文件夹”对话框。在其中添加数据来源服务器的原始文件夹，此文件夹中的数据将被复制到中心服务器中。

⑥ 单击“添加”按钮，显示如图 10-77 所示的“添加要复制的文件夹”对话框。

⑦ 单击“浏览”按钮，显示如图 10-78 所示的“选择文件夹”对话框。选择目标服务器中的文件夹，单击“确定”按钮。

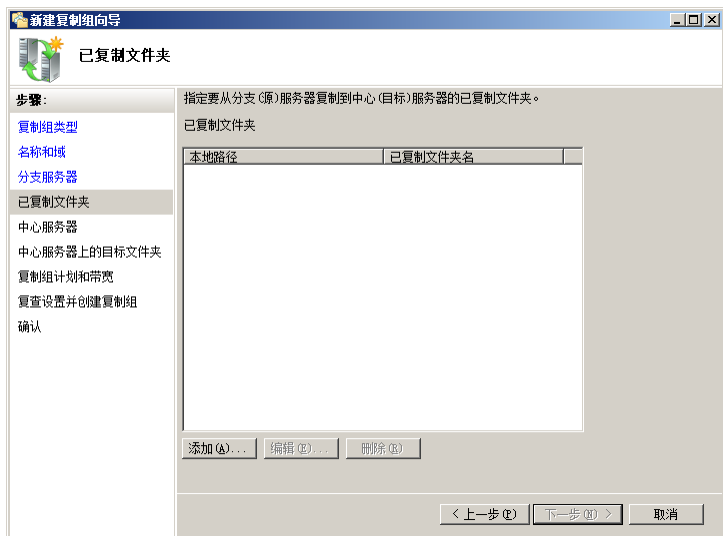


图 10-76 “已复制文件夹”对话框

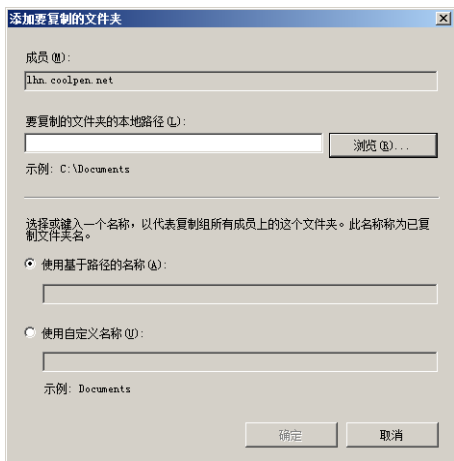


图 10-77 “添加要复制的文件夹”对话框



图 10-78 “选择文件夹”对话框

⑧ 单击“确定”按钮关闭“添加要复制的文件夹”对话框，返回“已复制文件夹”对话框，如图 10-79 所示。



图 10-79 “已复制文件夹”对话框

如果同一台服务器中有多个需要汇聚数据的文件夹，可重复上述操作。

⑨ 单击“下一步”按钮，显示如图 10-80 所示的“中心服务器”对话框。在“名称”文本框中键入保存数据的服务器名称，从其他服务器汇聚的数据将统一保存在该服务器中，网络管理员可以备份并且统一管理数据。

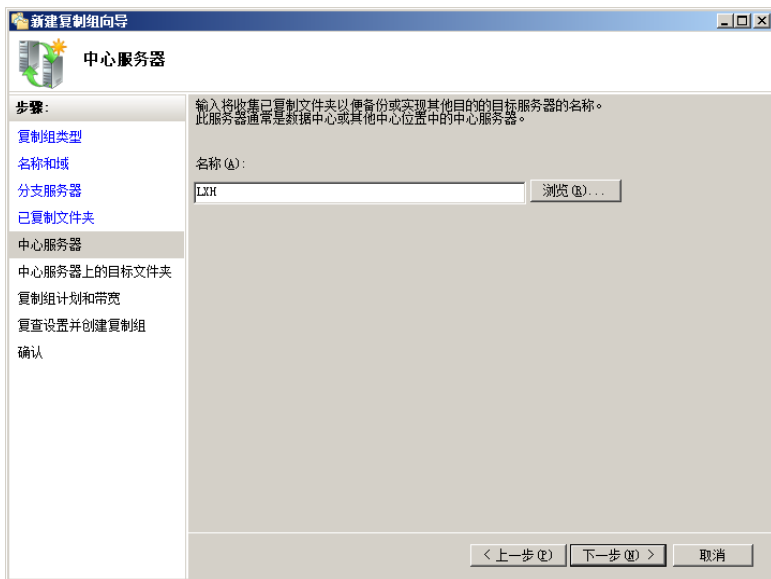


图 10-80 “中心服务器”对话框

⑩ 单击“下一步”按钮，显示如图 10-81 所示的“中心服务器上的目标文件夹”对话框。在“目标文件夹”文本框中键入中心服务器中存储 DFS 复制数据的目标文件夹路径，或者单击“浏览”按钮选择。

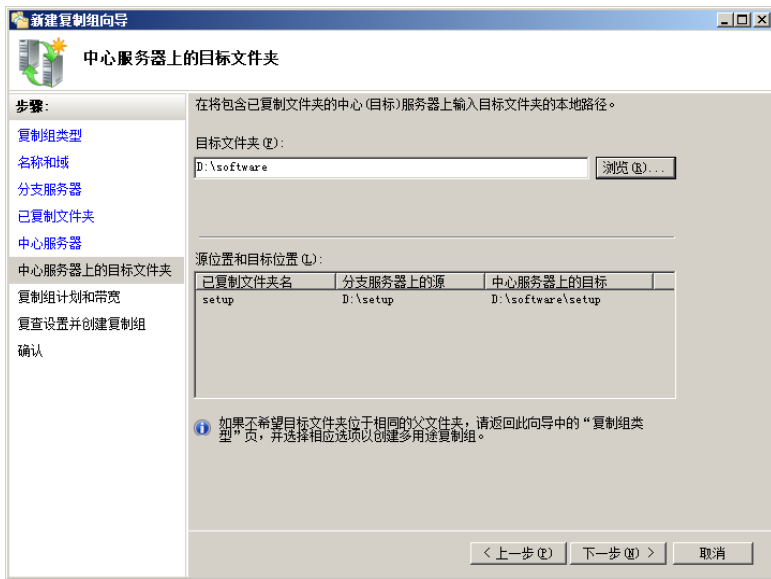


图 10-81 “中心服务器上的目标文件夹”对话框

⑪ 单击“下一步”按钮，显示如图 10-82 所示的“复制组计划和带宽”对话框，在其中根据企业实际情况定制复制的时间及复制频率。默认带宽设置为“完整”，即使用网络的最大传输流量，在每天的 24 小时不间断复制。

⑫ 单击“下一步”按钮，显示如图 10-83 所示的“复查设置并创建复制组”对话框，其中列出前面所做的设置。

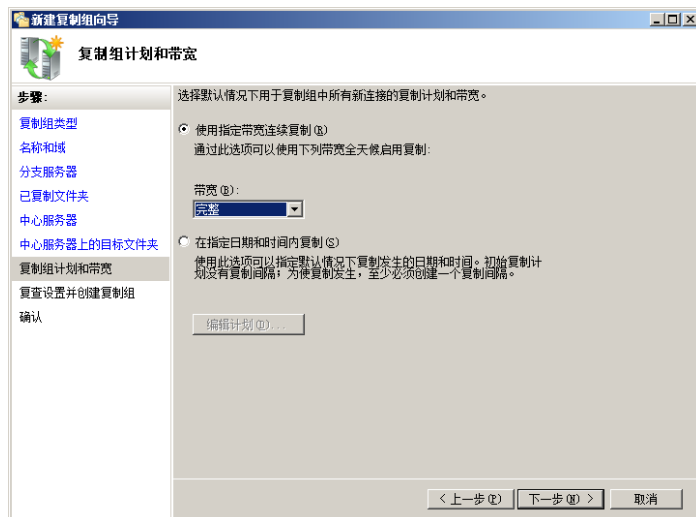


图 10-82 “复制组计划和带宽”对话框

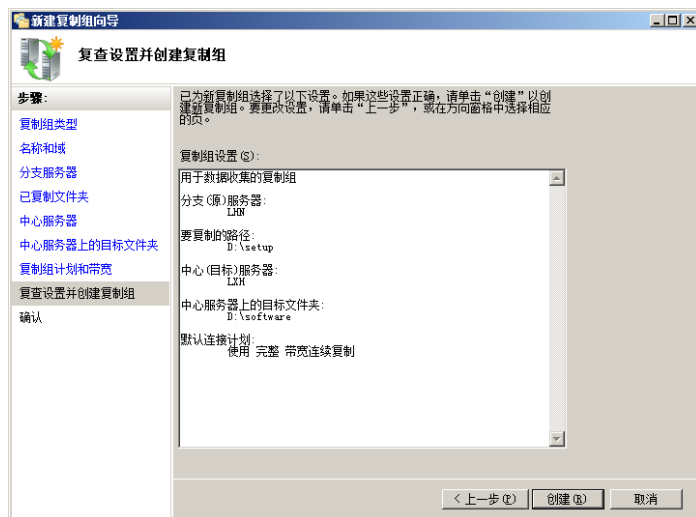


图 10-83 “复查设置并创建复制组”对话框

- ⑬ 单击“创建”按钮，开始创建复制组，创建完成后显示如图 10-84 所示的“确认”对话框。



图 10-84 “确认”对话框

- ⑭ 单击“关闭”按钮，显示如图 10-85 所示的“复制延迟”对话框。
- ⑮ 单击“确定”按钮，创建完成复制组，如图 10-86 所示。

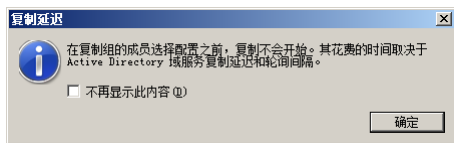


图 10-85 “复制延迟”对话框

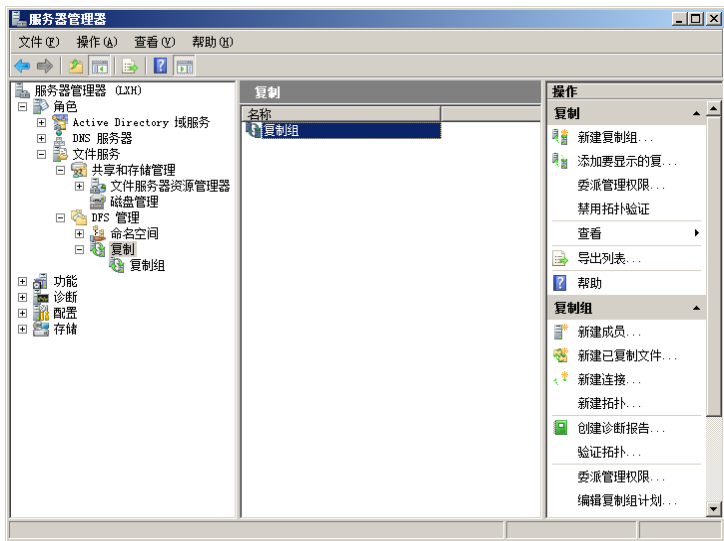


图 10-86 创建完成复制组

按照同样操作步骤可以将其他成员服务器添加到已经完成的 DFS 复制组中。

10.4 磁盘配额

Windows Server 2003/2008 提供了卷的磁盘配额功能，可以跟踪磁盘使用量的变化并控制磁盘空间的使用。磁盘配额是以文件所有权为基础的，只应用于卷，并且不受卷的文件夹结构及物理磁盘中的布局影响。它监视个人用户卷的使用情况，因此每个用户对磁盘空间的利用都不会影响同一卷中其他用户的磁盘配额。

10.4.1 磁盘配额的功能

在 Windows Server 2003/2008 系统中，系统管理员可以配置用户的磁盘配额。当用户超过所指定的磁盘空间限额时，阻止其进一步使用磁盘空间和记录事件；当用户超过指定的磁盘空间警告级别时记录事件。在第 1 种配置情况下，用户在使用磁盘时如果超过指定的磁盘空间，将无法使用；另外一种情况允许用户超额使用磁盘，但会将此情况记录在事件中。

也可以指定用户能超过其配额限度，如果不想拒绝用户访问卷，则需要跟踪每个用户的磁盘空间使用情况。启用配额，但不限制磁盘空间使用将非常有用。也可指定无论用户超过配额警告级别，还是配额限度时是否记录事件。

启用卷的磁盘配额时，磁盘配额不应用到现有的卷用户上。可以通过在“配额项目”窗口中添加新的配额项目，将磁盘空间配额应用到现有的卷用户上。

由于磁盘配额能够监视单个用户的卷使用情况，因此每个用户对磁盘空间的利用都不会影响同一卷中其他用户的磁盘配额。在用户看来，与在一个独立的磁盘卷中操作没有区别。

要支持磁盘配额，磁盘卷必须使用 NTFS 文件系统格式化，不受卷中用户文件的文件夹位置的限制。

10.4.2 设置磁盘配额

如果要在已经使用的磁盘中启用磁盘配额，Windows Server 2003 将计算到启动时间点为止在该卷中复制文件、保存文件或取得文件所有权的所有用户使用过的磁盘空间。然后根据计算结果，自动为

每个用户配额限度和警告级别。系统管理员可以为某个或多个用户设置不同的配额或禁用配额。另外，也可以为还没有在卷上复制文件、保存文件和取得文件所有权的用户设置配额，或者在一个新创建的卷中启用磁盘配额。

1. 启用磁盘限额

(1) 如果已经创建 NTFS 的卷，则可以在 Windows 资源管理器中右击要启动磁盘配额的卷。在快捷菜单中选择“属性”选项，打开“磁盘属性”对话框。

(2) 打开“配额”选项卡，选中“启用配额管理”复选框，如图 10-87 所示。

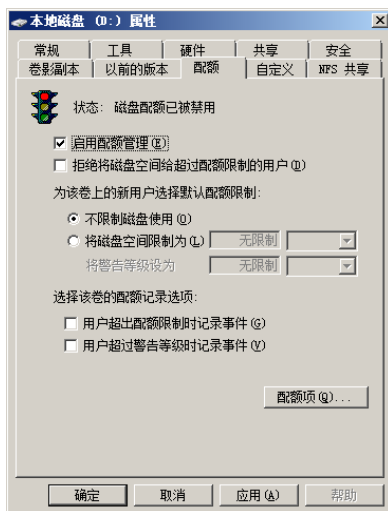


图 10-87 “配额”选项卡

其他选项如下。

拒绝将磁盘空间给超过配额限制的用户：选中该复选框，超过其配额限制的用户将收到来自 Windows 的“磁盘空间不足”错误信息，并且无法将额外的数据写入卷中。对于程序，会显示该卷已满。若未选中该复选框，则对用户写入数据的大小没有限制。

将磁盘空间限制为：选中该复选框，并输入允许卷的新用户使用的磁盘空间量，以及在将事件写入系统日志前已经使用的磁盘空间量。系统管理员可以在“事件查看器”中查看这些事件。在磁盘空间和警告级别中可以使用十进制数值（例如，20.5），并从下拉列表中选择适当的单位（如 KB、MB 及 GB 等）。

用户超出配额限制时记录事件：选中该复选框，如果启用配额，则只要用户超过其配额限制，事件就会写入到本地计算机的系统日志中，系统管理员可以在“事件查看器”中通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志。

用户超过警告等级时记录事件：选中该复选框，如果启用配额，则只要用户超过其警告级别，事件就会写入到本地计算机的系统日志中。系统管理员可以在“事件查看器”中通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志。

(3) 单击“确定”按钮保存所做设置，启用磁盘配额。

2. 为用户指定配额

为了使不同的用户可以使用不同大小的磁盘空间，可以为用户或组指定磁盘配额。

① 在“配额”选项卡中单击“配额项”按钮，显示如图 10-88 所示的配额项窗口。

② 单击“配额”→“新建配额项”选项，或单击工具栏中的“新建配额项”按钮，显示如图 10-89 所示的“选择用户”对话框。单击“高级”按钮，单击“立即查找”按钮，在“搜索结果”列表框中选择当前计算机中的用户。



图 10-88 配额项窗口

③ 选择要指定配额的用户后，单击“确定”按钮返回“选择用户”对话框。单击“确定”按钮，显示如图 10-90 所示的“添加新配额项”对话框。选中“将磁盘空间限制为”单选按钮，并在其后的文本框中为该用户设置访问磁盘的空间。需要注意的是，磁盘配额功能在共享及上传文件时都有效。即无论是在服务器上的共享文件夹中存放文件，还是通过 FTP 来上传文件，所有的文件总大小都不能超过磁盘限额所规定的空间数量。



图 10-89 “选择用户”对话框

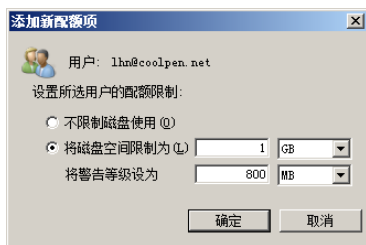


图 10-90 “添加新配额项”对话框

④ 单击“确定”按钮，保存所做设置。至此该磁盘配额的设置工作完成，指定的用户被添加到配额项列表中，如图 10-91 所示。

为用户设置磁盘配额以后，在配额项窗口中即可监视每个用户的磁盘配额使用情况。如果用户需要删除指定的配额项，可右击并从快捷菜单中选择“删除”选项。

如果要更改某一个用户的磁盘配额设置，可右击该用户。选择快捷菜单中的“属性”选项，显示如图 10-92 所示的配额设置对话框。

使用指定配额项的优点如下。

- (1) 登录到相同计算机的多个用户不干涉其他用户的工作能力。
- (2) 一个或多个用户不独占公用服务器上的磁盘空间。
- (3) 在个人计算机的共享文件夹中，用户不使用过多的磁盘空间。



图 10-91 添加指定配额项用户



图 10-92 配额设置对话框

10.5 脱机文件与数据同步

对于移动用户而言，由于往往需要将笔记本电脑带回家中或者在出差时随身携带，因此会切断与文件服务器的连接，从而无法读取保存在文件服务器中的文件和数据。同时修改笔记本电脑中的文档以后，也往往忘记将其保存到服务器，从而导致文件服务器与笔记本电脑中所保存的文件版本不同。借助脱机文件和数据同步，可以很好地解决这些问题。

10.5.1 设置服务端的脱机文件

为了使共享网络资源可以脱机使用，“脱机文件”将这些共享资源的一个版本存储在客户端的文件系统中缓存，文件缓存实际上是一部分保留的磁盘空间。无论是否连接到网络，客户端都可以访问这种缓存。创建新的共享资源时，默认情况下允许脱机访问，这意味着可以在有潜在不安全因素的计算机中脱机存储安全的共享资源。如果要获得最佳的安全性，则不要允许用户脱机存储文件。当然用共享权限或访问控制来设置合适的权限，也可以在很大程度上提高安全性。

在“服务器管理器”窗口中展开“角色”→“文件服务”选项，选中“共享和存储管理”选项，在中间区域右击要设置同步的共享文件夹。选择快捷菜单中的“属性”选项，显示如图 10-93 所示的共享文件夹属性对话框。



图 10-93 共享文件夹的属性对话框

单击“高级”按钮，打开“高级”对话框即可设置脱机文件。具体设置请参见前面相关内容，这里不再赘述。

10.5.2 Windows XP/2003 客户端的脱机文件设置与同步

借助脱机文件，即使未与网络连接，也可以使用网络文件和程序。只需将共享文件夹设置为脱机文件，当用户的笔记本电脑离开企业网络或者网络连接发生故障时也可以像往常一样继续工作，访问这些文件和文件夹的权限与先前连接到网络时相同。当连接状态变化时，脱机文件图标将出现在通知区域中，显示一个提示气球通知用户连接已经发生变化。

1. 创建脱机使用

① 将要同步的共享文件夹映射为网络驱动器，具体操作方法请参照“映射网络驱动器”中的有关内容。

② 右击要实现数据同步的网络驱动器，在快捷菜单中选择“允许脱机使用”选项运行“脱机文件向导”。单击“下一步”按钮，显示如图 10-94 所示的设置同步时机对话框，选中“登录和注销时自动同步处理脱机文件”复选框，将在当前用户登录至域或从域中注销时自动对脱机文件实施同步操作。

提示

为了确保客户端与文件服务器的中文件保持一致，建议选中该复选框，同步时机也可以稍后在“同步管理器”中设置。

默认状态下，设置映射网络驱动器之后快捷菜单中不会显示“允许脱机使用”选项。用户必须首先打开“控制面板”中的“文件夹选项”对话框，打开如图 10-95 所示的“脱机文件”选项卡。选中“启用脱机文件”复选框，然后根据需要设置其后的选项，也可以保持系统默认。

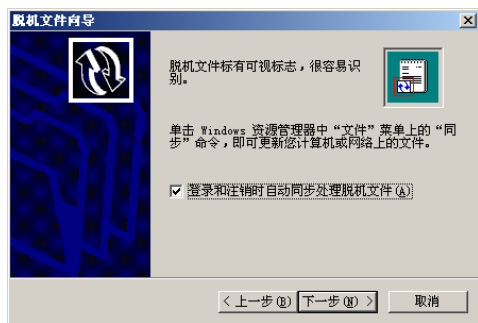


图 10-94 设置同步时机对话框

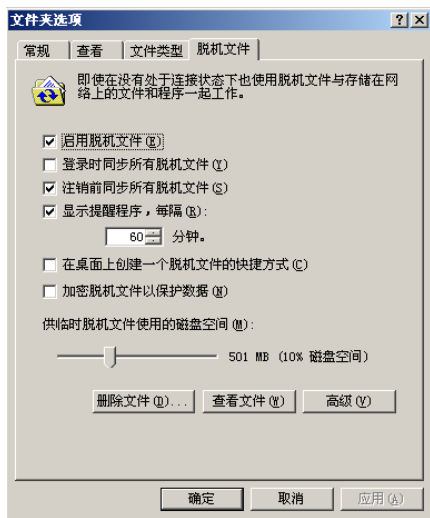


图 10-95 “脱机文件”选项卡

③ 单击“下一步”按钮，显示如图 10-96 所示的设置启用提醒对话框。当计算机脱机工作时，将每隔一段时间出现一条消息，提醒用户当前未与企业网络连接。

提示

如果是暂时离开企业网络，可以选中该复选框，以提示用户尽快与文件服务器同步；如果是长时间脱机，那么频繁的提示将徒增烦恼并影响正常工作。

④ 单击“完成”按钮，即可开始同步。如果当前共享文件夹中包含子文件夹，则显示如图 10-97 所示的“确认脱机子文件夹”对话框。选择“是，让该文件夹及其所有子文件夹都可以脱机使用”单选按钮，该共享文件夹中的所有子文件夹和文件都可以实现脱机和同步，建议选择该选项；如果选中

“否，只让该文件夹可以脱机使用”单选按钮，那么子文件夹中的文件将无法实现脱机和同步。

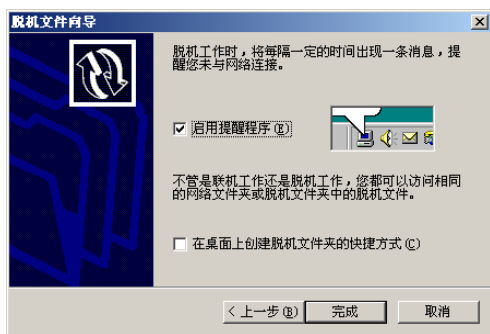


图 10-96 设置启用提醒对话框

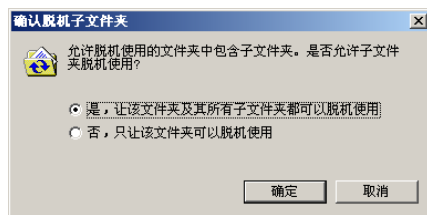


图 10-97 “确认脱机子文件夹”对话框

⑤ 单击“确定”按钮，即可将其包含的所有子文件夹实现脱机使用。根据共享资源占据磁盘空间的大小，同步所需的时间也会有所不同。

2. 设置脱机共享文件

创建脱机文件之后，还可以设置本地计算机中已经创建的所有脱机文件，操作步骤如下。

① 在 Windows 资源管理器中单击“工具”→“同步”选项，打开如图 10-98 所示的“要同步的项目”对话框。在“选择要同步的项目”列表框中选中要同步的共享文件夹前的复选框，单击“同步”按钮，即可立即实现本地计算机与网络共享文件的数据同步。

② 单击“设置”按钮，显示“同步设置”对话框。默认为“登录/注销”选项卡，如图 10-99 所示，在其中设置用户在“登录计算机”或/和“从计算机注销”时与哪些远程共享文件夹自动实现数据同步。

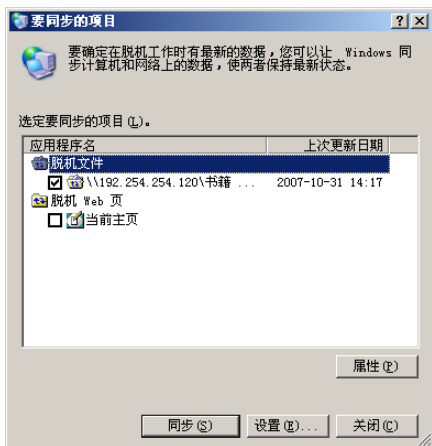


图 10-98 “要同步的项目”对话框

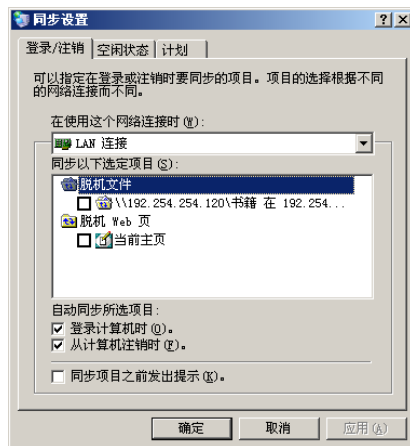


图 10-99 “登录/注销”选项卡

③ 打开“空闲状态”选项卡，如图 10-100 所示。选中“在计算机空闲时同步所选项目”复选框，设置在计算机空闲时，而不是在登录或从计算机注销时实现数据同步。当共享文件夹中的数据量较大时，同步需要较长的时间。因此在离开座位，即计算机空闲时同步数据，无疑是一种非常好的选择。

提示 可以使用多种不同的组合将这些选项应用到每个共享资源的脱机文件中。

④ 打开“计划”选项卡，即可查看“当前同步任务”。默认为空，单击“添加”按钮即可启动“同步计划向导”。在如图 10-101 所示的对话框中选择实现同步的网络连接，以及要同步的共享文件夹。

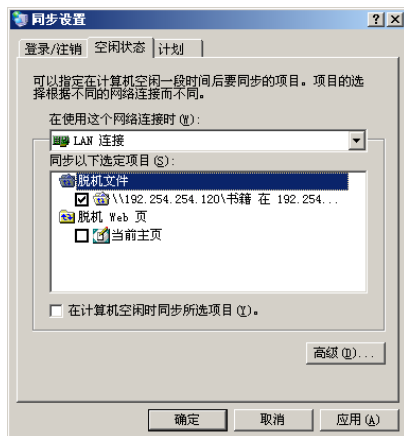


图 10-100 “空闲状态”选项卡



图 10-101 选择连接与脱机文件夹

⑤ 单击“下一步”按钮，显示如图 10-102 所示的对话框，设置同步开始的时间、日期，以及时机。

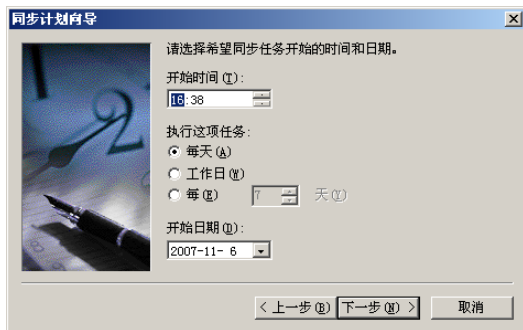


图 10-102 设置脱机文件的同步时间等

提示



用户可以手动启动同步，也可以设置“同步管理器”来控制脱机文件与网络同步的时间。脱机文件可以控制执行完全同步，还是快速同步。完全同步可以确保获得每个指定为允许脱机使用的网络文件的最新版本；快速同步比完全同步速度快得多，但是可能不提供每个指定为可以脱机使用的网络文件的最新版本。不过，快速同步可以确保获得每个文件的完整版本，使用户能够继续工作。

➤➤ 10.5.3 Windows Vista/2008 客户端脱机文件的加密与同步

1. 启用脱机文件功能

如果在 Windows Vista/2008 客户端使用脱机文件，则执行如下操作。

- ① 单击“开始”→“控制面板”选项，打开“控制面板”窗口，如图 10-103 所示。

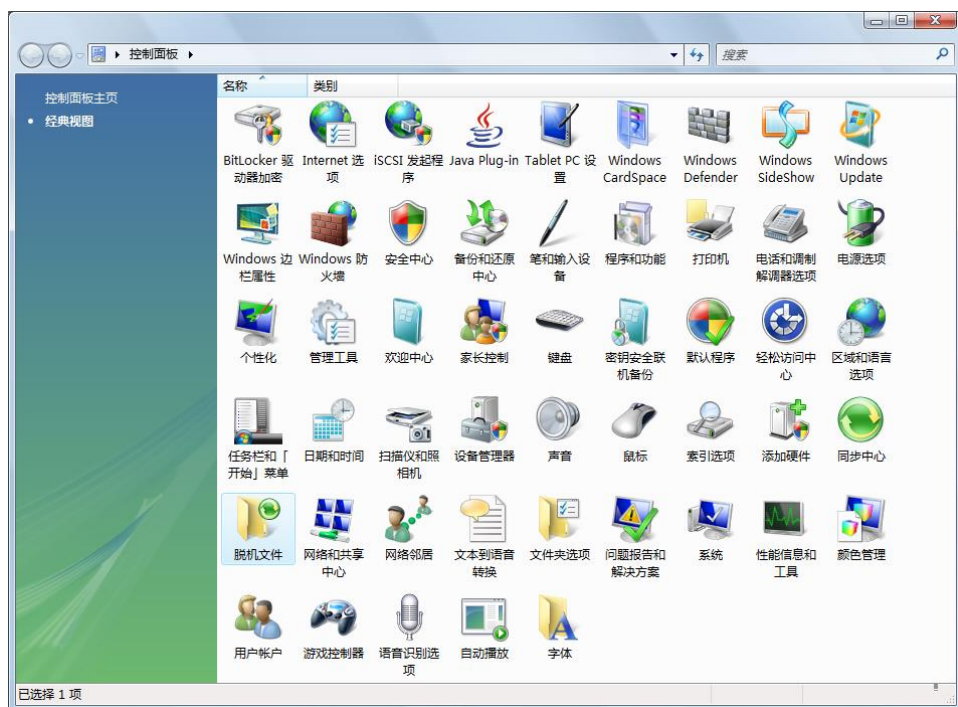


图 10-103 “控制面板”窗口

- ② 双击“脱机文件”图标，打开如图 10-104 所示的“脱机文件”对话框，提示当前已启用脱机文件功能。

如果没有启用，则单击“启用脱机文件”按钮，并重新启动该计算机以激活脱机文件。

2. 同步脱机文件

- ① 单击“开始”→“计算机”选项，打开“计算机”窗口。单击“工具”→“映射网络驱动器”选项，打开如图 10-105 所示的“映射网络驱动器”对话框。在“驱动器”下拉列表框中选择所映射的网络驱动器。在“文件夹”文本框中键入共享文件夹的网络路径，或单击“浏览”按钮选择。

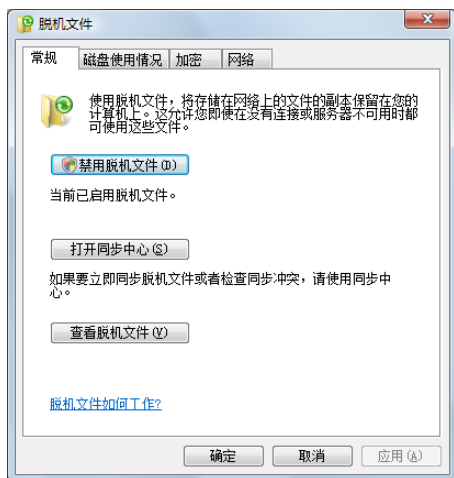


图 10-104 “脱机文件”对话框

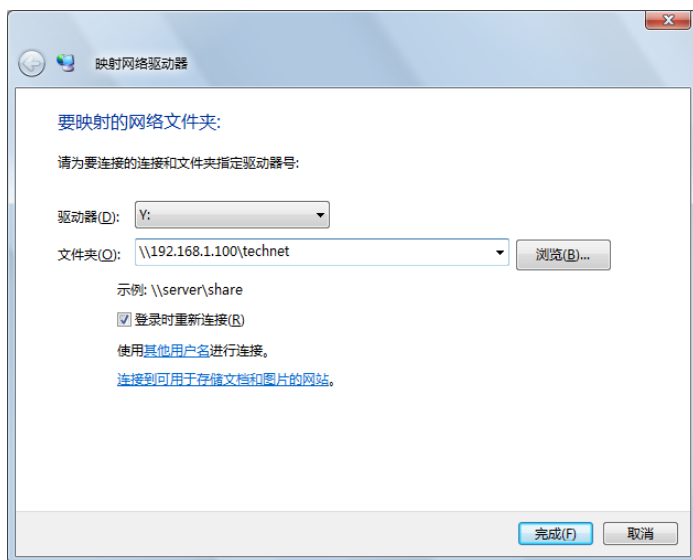


图 10-105 “映射网络驱动器”对话框

- ② 单击“确定”按钮，完成网络驱动器的映射。

③ 右击映射的网络驱动器，在快捷菜单中选择“同步”选项，可立即执行同步操作；选择“始终脱机可用”选项，可以在任何情况下使用映射驱动器的文件。

3. 加密脱机文件

脱机文件是存储在计算机中的网络文件副本，可以在无法连接到网络或包含文件的网络文件夹时访问脱机文件。默认情况下，文件不会加密。如果脱机文件包含敏感或机密信息，并且用户希望通过限制脱机文件的访问来使其更安全，则需要加密这些脱机文件。加密脱机文件会为用户提供了额外的访问保护级别，该访问保护级别与 NTFS 文件系统权限无关。这种文件可以帮助用户在计算机丢失或被盗时保护文件的安全。

- ① 在“控制面板”窗口中双击“脱机中心”图标，打开“脱机文件”窗口。
- ② 打开如图 10-106 所示的“加密”选项卡，提示当前没有加密。
- ③ 单击“加密”按钮，加密脱机文件，如图 10-107 所示。根据脱机文件的多少，加密所使用的时间也不同。

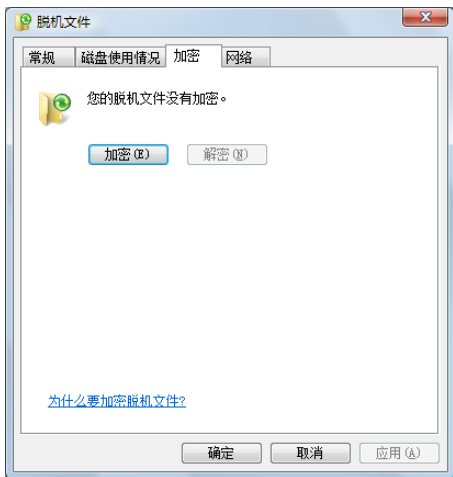


图 10-106 “加密”选项卡

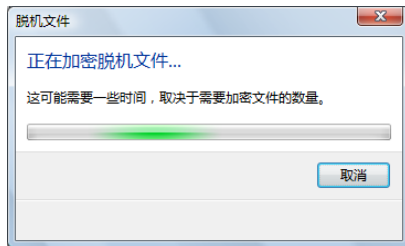


图 10-107 加密脱机文件

10.6 实现软 RAID

文件服务器通过利用 RAID 来实现磁盘阵列，从而实现大容量且高速存储。硬件 RAID 解决方案速度快且稳定性好，可以有效地提高硬盘的可用性和冗余度，但其价格也居高不下。Windows Server 2003/2008 提供了内嵌的软件 RAID 功能，可以实现 RAID-0、RAID-1 及 RAID-5。软 RAID 不仅实现上非常方便，而且还可以节约很多资金。当然，软 RAID 的性能和效率也不能与硬 RAID 同日而语。

10.6.1 卷与 RAID

卷是 Windows Server 2003/2008 的数据存储单元，Windows Server 2003/2008 支持 5 种类型的动态卷，即简单卷、跨区卷、带区卷、镜像卷和 RAID-5 卷，并且每一种卷对应一种 RAID 类型。其中镜像卷和 RAID-5 卷具有容错功能，也称为“容错卷”。

1. 卷类型

(1) 简单卷

简单卷由单个物理磁盘上的磁盘空间组成，即由磁盘上的单个区域或者链接在一起的相同磁盘上的多个区域组成。可以在同一磁盘中扩展简单卷或将其扩展到其他磁盘，如果跨多个磁盘扩展简单卷，则该卷就是跨区卷。



(2) 带区卷

带区卷通过将两个或更多磁盘上的可用空间区域合并到一个逻辑卷创建，它使用 RAID-0，从而可以在多个磁盘上分布数据。带区卷不能被扩展或镜像，并且不提供容错。如果包含带区卷的其中一个磁盘出现故障，则整个卷无法工作。当创建带区卷时，最好使用相同大小、型号和制造商的磁盘。

利用带区卷可以将数据分块，并且按照一定的顺序在阵列中的所有磁盘中分布数据，与跨区卷类似。带区卷可以同时对所有磁盘执行写数据操作，从而以相同的速率在所有磁盘中写数据。

提示



尽管不具备容错能力，但带区卷在所有 Windows 磁盘管理策略中的性能最好，同时它通过可在多个磁盘中分配 I/O 请求而提高了 I/O 性能。

(3) 跨区卷

跨区卷是将来自多个磁盘的未分配空间合并到一个逻辑卷中，以便更有效地使用多个磁盘系统中的所有空间和所有驱动器号。用于创建跨区卷的未分配空间区域的大小可以不同，它可以快速增加卷的空量。但不能提高对磁盘数据的读取性能，也不具备容错功能。

需要注意的是，在更改跨区卷之前，应首先备份其中的所有信息。另外，跨区卷不能是镜像卷并且不提供容错。如果包含一个跨区卷的磁盘出现故障，则整个卷将无法工作，并且其中的数据都将丢失。

(4) 镜像卷

利用镜像卷，即 RAID-1 卷可以将用户的相同数据同时复制到两个物理磁盘中。如果一个物理磁盘出现故障，虽然该磁盘中的数据将无法使用，但系统能够继续使用尚未损坏的磁盘读写数据。并通过另一磁盘上保留完全冗余的副本，保护磁盘中的数据免受介质故障的影响。

要创建镜像卷，必须使用另一磁盘中的可用空间。动态磁盘中现有的任何卷（甚至是系统卷和引导卷）都可以使用相同，或不同的控制器镜像到其他磁盘上大小相同或更大的另一个卷。最好使用大小、型号和制造厂家均相同的磁盘作为镜像卷，以避免可能产生的兼容性错误。

镜像卷可以增强读性能，因为容错驱动程序同时从两个成员中读取数据，所以读取数据的速度会有所增加。当然由于容错驱动程序必须同时向两个成员写数据，所以写入性能会略有降低。

镜像卷可包含任何分区（包括启动分区或系统分区），但是其中的两个硬盘都必须是 Windows Server 2003 动态磁盘。

(5) RAID-5 卷

在 RAID-5 卷中，Windows Server 2003 通过为该卷的每个硬盘分区中添加奇偶校验信息带区实现容错。如果某个硬盘出现故障，Windows Server 2008 则用其余硬盘中的数据和奇偶校验信息重建发生故障的硬盘中的数据。

由于要计算奇偶校验信息，所以 RAID-5 卷的写操作要比镜像卷慢一些。但是 RAID-5 卷比镜像卷提供更好的读性能，原因是 Windows Server 2008 可以从多个盘中同时读取数据。与镜像卷相比，RAID-5 卷的性价比较高。而且其中的硬盘数量越多，冗余数据带区的成本越低，因此被广泛应用于数据的存储。

2. 查看卷状态

在“磁盘管理”窗口中可以查看卷的状态，如图 10-108 所示。例如失败、失败的重复、格式化及正常等，了解这些状态信息代表的含义对日后处理卷故障会有很大的帮助。

(1) 失败

当基本或动态卷无法自动启动或磁盘损坏时，就会出现“失败”状态。当导入带有“不完整的数据”状态的卷时，也会显示该状态，在出现故障的卷上将显示错误图标。在修复磁盘或文件系统之前，“失败”状态表示数据丢失。

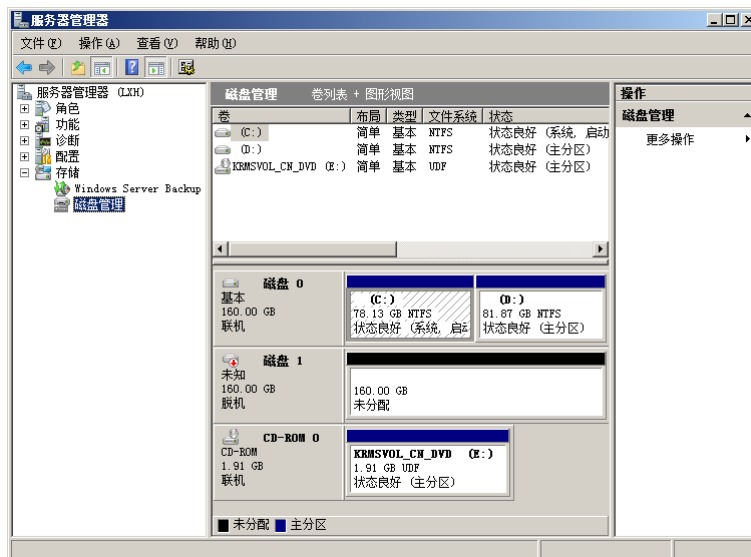


图 10-108 卷状态

如果是基本卷，要确保基本物理磁盘已正确插入或连接到计算机；如果是动态磁盘，要确保基本动态物理磁盘已联机；如果动态磁盘已返回到“联机”状态，但动态卷尚未返回到“正常”状态，这时可以通过手动重新激活该卷；如果使用带有旧数据的镜像卷或 RAID-5 卷，则基本磁盘联机不能自动重新激活卷；如果包含当前数据的磁盘已断开连接，则应首先使这些磁盘联机（允许数据同步）。

（2）失败的重复

当镜像卷或 RAID-5 卷中的数据由于某个基本磁盘未联机而不再具有容错能力时，就会出现“失败的重复”状态。在带有“失败的重复”的卷上将显示警告图标。

带有“失败的重复”状态的卷经常会显示相关的子状态（包含在圆括号中），每个卷同时显示一种子状态。子状态的显示顺序将取决于它们在表 10-2 中的出现顺序。例如，如果只有一个卷作为启动卷、系统卷、活动卷、页面文件和故障转储，则其状态显示为“失败的重复（系统）”。然而如果镜像卷或 RAID-5 卷出现错误，则将优先显示“（有危险）”子状态。

表 10-2 子状态的显示顺序

失败的重复（子状态）	描 述
系统	表明该卷是系统卷
启动	表明该卷是启动卷
页面文件	表明该卷包含有页面文件
故障转储	表明该卷包含有故障转储，也称为“内存转储”，可用于在 Windows NT 操作系统意外停止时记录系统内存的内容
有危险	表明由于某个磁盘出现故障且剩余动态磁盘检测到了 I/O 错误，镜像卷或 RAID-5 卷上的数据不再具有容错能力。只要在磁盘上的任一部分检测到 I/O 错误，则磁盘的所有动态卷上都将显示警告图标，不具备容错能力的动态卷将显示“良好（有危险）”状态

（3）格式化

“格式化”状态是一种只在使用文件系统格式化卷时才出现的临时状态，格式化卷时将以百分比显示格式化卷的进度，格式化完成后卷状态将变为“正常”状态。

（4）正常

“正常”状态是基本卷和动态卷的正常状态，可以访问处于该状态的卷。并且没有已知问题，不需要用户操作。

带有“正常”状态的卷经常会显示相关的子状态（包含于圆括号中），每个卷一次只能显示一种子

状态，子状态的显示顺序将取决于它们在表 10-3 中的出现顺序。例如，如果只有一个卷作为启动卷、系统卷、活动卷、页面文件和故障转储，则其状态显示为“正常（系统）”，然而如果动态卷出现错误，则优先显示“（有危险）”子状态。

表 10-3 子状态的显示顺序

良好（子状态）	描 述
系统	表明该卷是系统卷
启动	表明该卷是启动卷
页面文件	表明该卷包含有页面文件
活动	表明该卷是基本磁盘上的活动卷
故障转储	表明该卷包含有故障转储，也称为“内存转储”，可用于在 Windows NT 操作系统意外停止时记录系统内存的内容
休眠分区	表明该卷是原始设备生产商（OEM）休眠分区，可用于保存某些笔记本电脑在休眠期间的系统当前状态
GPT 保护分区	在基于 x86 的计算机上，表明卷是 GUID 分区表（GPT）磁盘。GPT 可保护分区包含保护 MBR 以防止基于 x86 计算机上的磁盘工具意外破坏 GPT 分区
EFI 系统分区	表明卷是 GPT 磁盘上的可扩展固件接口（EFI）系统分区
EISA 配置	表明该卷是原始设备生产商（OEM）分区
未知分区	表明没有识别该分区。带有“良好（未知分区）”状态的主启动记录（MBR）或 GUID 分区表（GP）磁盘上的分区可能是不可识别的设备制造商（OEM）分区或非 Windows 操作系统分区。不能格式化带有“良好（未知分区）”状态的分区或为其指派驱动器号或装入点，也不能访问其上的数据。不过，可以使用“磁盘管理”或 DISKPART 命令删除这些分区
有危险	该动态卷目前可以访问，但是基础动态磁盘上检测到 I/O 错误。如果动态磁盘的任何部分检测到 I/O 错误，则该磁盘的所有卷都将显示“正常（有危险）”状态，同时在该卷上显示警告图标

（5）正在重新产生

当重新激活 RAID-5 卷中的丢失磁盘、重新激活 RAID-5 卷中的脱机磁盘、重新激活出现故障的 RAID-5 卷、导入 RAID-5 卷中的磁盘，并且为 RAID-5 卷重新生成数据和奇偶校验时，将出现“正在重新产生”状态。不需要用户操作。重新生成完成后，卷将返回到“正常”状态。在重新生成数据和奇偶校验的过程中，可以访问 RAID-5 卷。

（6）重新同步

当创建镜像或重新启动带有镜像卷的计算机、重新激活镜像卷中的脱机磁盘、导入镜像卷中的磁盘，以及正在重新同步镜像卷时，将出现“重新同步”状态。从而使两个镜像包含相同的数据，不需要用户操作。重新同步完成后，镜像卷将返回到“正常”状态。重新同步可能需要一些时间，具体取决于镜像卷的大小。尽管在重新同步的过程中可以访问镜像卷，但是应该避免在重新同步的过程中更改配置（例如中断镜像）。

（7）未知

当卷的引导扇区损坏（可能是病毒所致）且无法访问该卷中的数据时，便会出现“未知”状态。

导入磁盘时，磁盘上的所有卷将在“外部磁盘卷”对话框中显示“正常”状态；除非这些卷出现问题。导入镜像卷或 RAID-5 卷时，可能出现的问题是“不完整的数据”、“数据没有重复”或“陈旧数据”。

（8）不完整的数据

当数据跨越多个磁盘并有部分磁盘已移走时，将会在“外部磁盘卷”对话框中显示“不完整的数据”状态。除非在移动完包含此卷的其余磁盘后，同时导入了所有磁盘；否则该卷中的数据将被破坏。以后将不能导入丢失的磁盘以还原数据。

（9）数据没有重复

当镜像卷或 RAID-5 卷中的磁盘只有一个没有被导入时，会在“外部磁盘卷”对话框中显示“数据没有重复”状态。在“磁盘管理”窗口中镜像卷的导入部分将接收到“失败的重复”状态，而包含

镜像未导入部分的磁盘将接收到“丢失”状态，RAID-5 卷将接收到“失败的重复”状态。

要防止“数据没有重复”状态的发生，将所有属于镜像卷或 RAID-5 卷的磁盘同时连接到计算机，然后同时导入所有磁盘。对于镜像卷，可在以后导入“丢失”的磁盘以还原冗余。

(10) 陈旧数据

当镜像卷或 RAID-5 卷具有陈旧的镜像信息、陈旧的奇偶校验信息或 I/O 错误时，就会在“外部磁盘卷”对话框中显示“陈旧数据”状态。

10.6.2 动态磁盘

安装 Windows Server 2008 时，硬盘自动初始化为基本磁盘。如果创建新卷集、条带集或者 RAID-5 卷，则必须转换成动态磁盘。

磁盘从基本磁盘转换为动态磁盘后磁盘中包含的将是卷，而不再是磁盘分区，每个卷是硬盘驱动器上的一个逻辑部分。可以为每个卷指定一个驱动器字母或者挂接点，只能在动态磁盘中创建卷。动态磁盘优于基本磁盘的特点如下。

(1) 卷可以扩展到包含非邻接的空间，这些空间可以在任何可用的磁盘上。

(2) 每个磁盘中可以创建的卷的数目没有限制。

(3) Windows Server 2008 将动态磁盘配置信息存储在磁盘上，而不是存储在注册表中或者其他位置。在这些位置，这些信息不能被准确地更新。Windows Server 2003 将这些磁盘配置信息复制到所有其他动态磁盘中，这样单个磁盘的失灵将不会影响访问其他磁盘中的数据。

1. 磁盘初始化

新安装的磁盘，必须经过初始化才能使用，而且初始化后会转换成基本磁盘。

① 打开“服务器管理器”窗口，依次展开“存储”→“磁盘管理”选项，显示计算机中安装的所有磁盘，如图 10-109 所示。

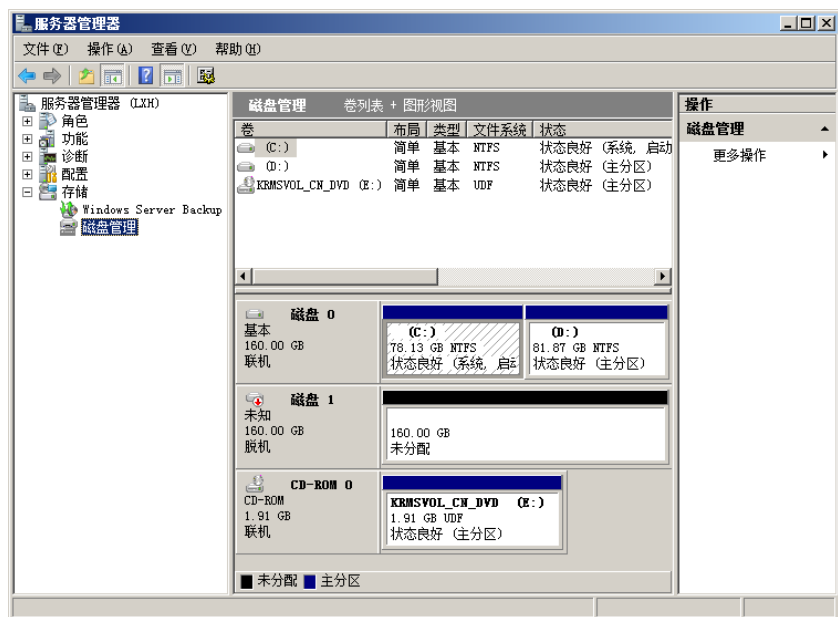


图 10-109 安装的所有磁盘

② 新安装的磁盘尚未联机，右击新安装的磁盘，在快捷菜单中选择“联机”选项使其联机。

③ 再次右击新安装的磁盘，选择快捷菜单中的“初始化磁盘”选项，显示如图 10-110 所示的“初始化磁盘”对话框。在“选择磁盘”列表框中选择要初始化的磁盘，即新安装的磁盘。

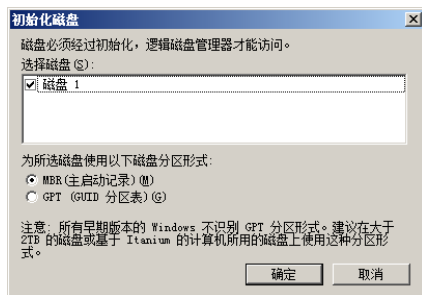


图 10-110 “初始化磁盘”对话框

- ④ 单击“确定”按钮，磁盘初始化完成。并且变为基本磁盘，如图 10-111 所示。

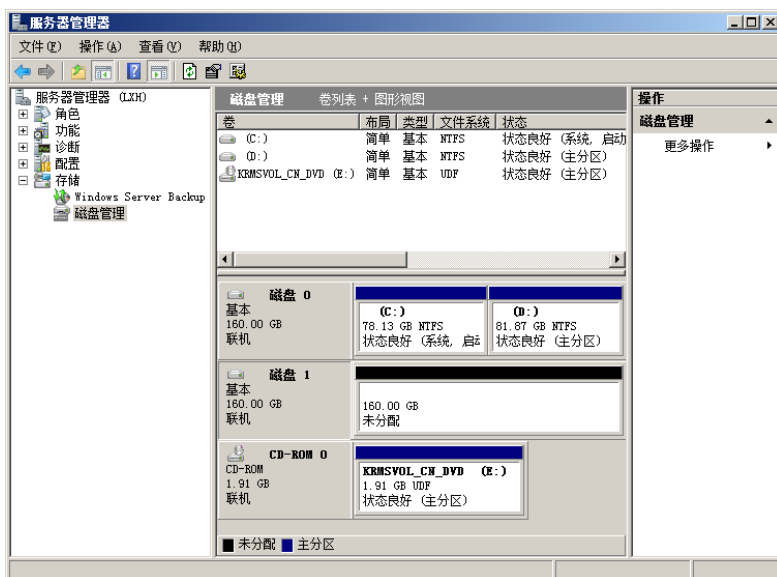


图 10-111 基本磁盘

2. 从基本磁盘升级到动态磁盘

- ① 选择基本磁盘，右击并选择快捷菜单中的“转换到动态磁盘”选项。显示如图 10-112 所示的“转换为动态磁盘”对话框，选择要转换成动态磁盘的基本磁盘。
- ② 单击“确定”按钮，磁盘转换完成，原来的基本磁盘转换为动态磁盘，如图 10-113 所示。

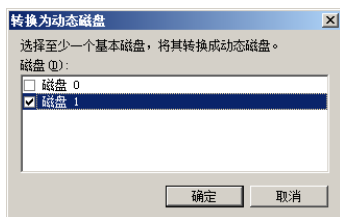


图 10-112 升级到动态磁盘



提示

从基本磁盘转换为动态磁盘后，如果动态磁盘中存储有数据，则不能转换回基本磁盘；除非删除所有卷。

需要注意的是，在升级到动态磁盘时应当注意以下问题。

- ① 将基本磁盘升级到动态磁盘后，不能将动态卷转换回基本卷；除非删除磁盘中的所有动态卷，然后使用“还原为基本磁盘”命令。

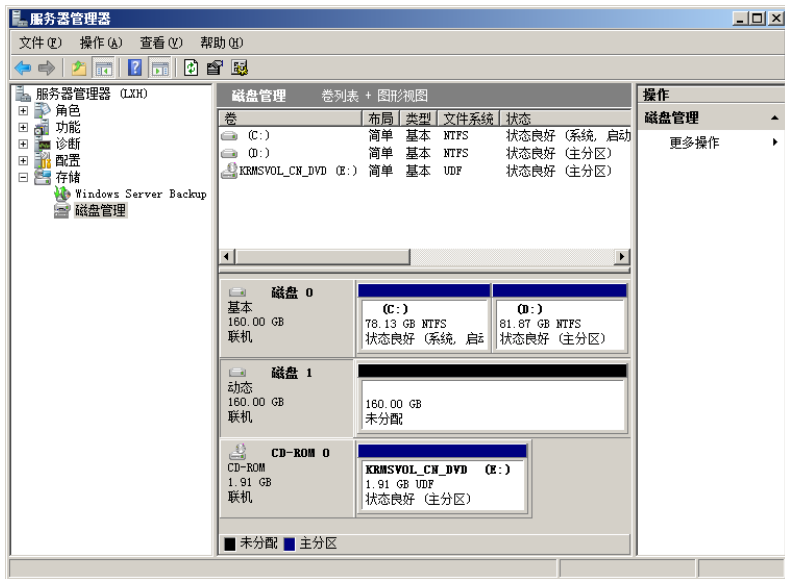


图 10-113 转换为动态磁盘

- ② 在升级磁盘之前，关闭在其中运行的程序。
- ③ 为保证升级成功，任何要升级的磁盘都必须至少包含 1 MB 的未分配空间。在磁盘中创建分区或卷时，“磁盘管理”将自动保留这个空间，但是带有其他操作系统创建的分区或卷的磁盘上可能没有这个空间。
- ④ 扇区大小超过 512 个字节的磁盘不能从基本磁盘升级为动态磁盘。
- ⑤ 一旦升级，动态磁盘就不能包含分区或逻辑驱动器，也不能被非 Windows Server 2003/2008 操作系统访问。

10.6.3 实现软 RAID

软 RAID 也必须得多磁盘系统中才能实现。实现 RAID-1 最少要拥有两个硬盘，实现 RAID-5 最少要拥有 3 个硬盘。通常情况下，操作系统所在磁盘采用 RAID-1，而数据所在磁盘采用 RAID-5。

这里以创建 RAID-5 卷为例，操作步骤如下。

- ① 在“磁盘管理”窗口中右击要设置软 RAID 的硬盘。在快捷菜单中选择“新建 RAID-卷”选项，打开“新建 RAID-5 卷向导”对话框，如图 10-114 所示。

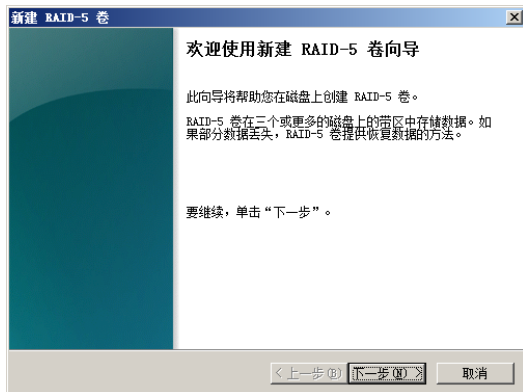


图 10-114 “新建 RAID-5 卷向导”对话框

- ② 单击“下一步”按钮，显示如图 10-115 所示的“选择磁盘”对话框。在“可用”列表框中选择要创建为 RAID-5 卷的磁盘，单击“添加”按钮添加到右侧“已选的”列表框中，并在“选择空间

量”文本框中设置磁盘空间的大小。

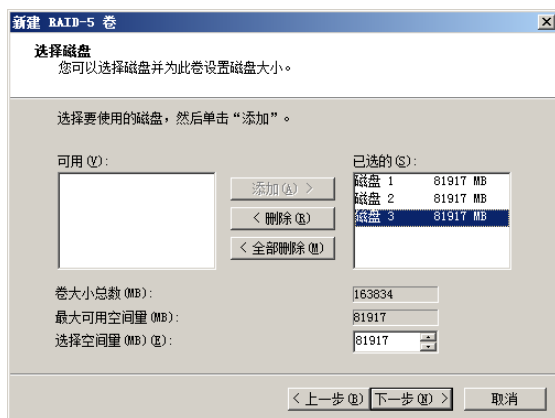


图 10-115 “选择磁盘”对话框

③ 单击“下一步”按钮，显示如图 10-116 所示的“分配驱动器号和路径”对话框。在“分配以下驱动器号”下拉列表框中选择一个驱动器盘符，以便于管理和访问。

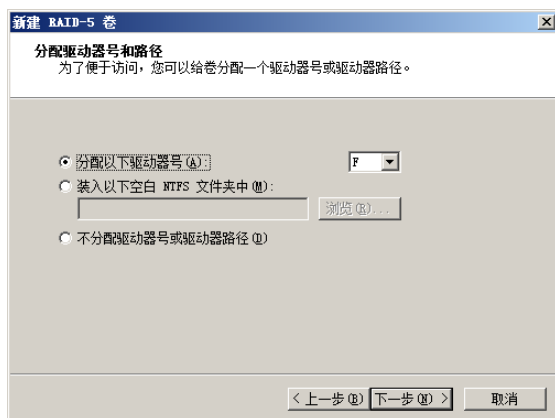


图 10-116 “分配驱动器号和路径”对话框

④ 单击“下一步”按钮，显示如图 10-117 所示的“卷区格式化”对话框。选择“按下面设置格式化这个卷”单选按钮，并采用默认的 NTFS 文件系统和分配单位大小。选中“执行快速格式化”复选框，以加快格式化速度。

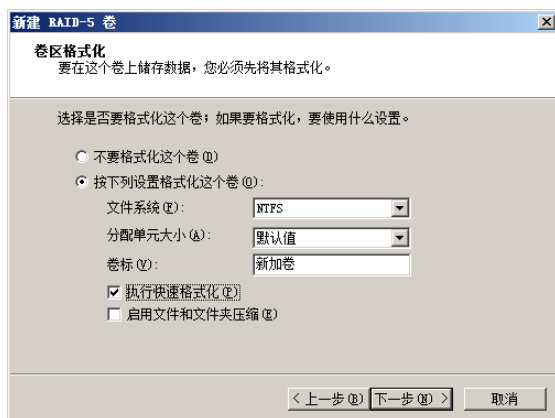


图 10-117 “卷区格式化”对话框

⑤ 单击“下一步”按钮，显示如图 10-118 所示的“正在完成新建 RAID-5 卷向导”对话框，其中列出前面所做的配置。

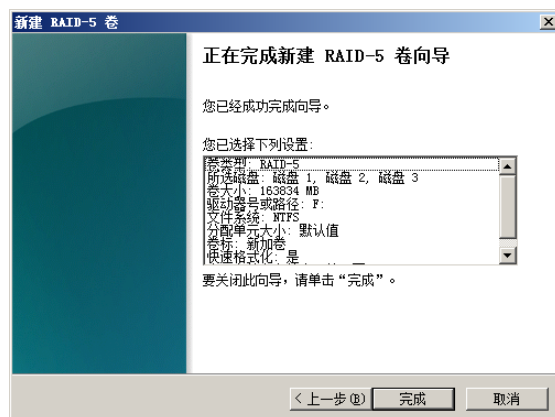


图 10-118 “正在完成新建 RAID-5 卷向导”对话框

- ⑥ 单击“完成”按钮，RAID-5 卷创建完成，如图 10-119 所示，系统自动格式化新创建的卷。

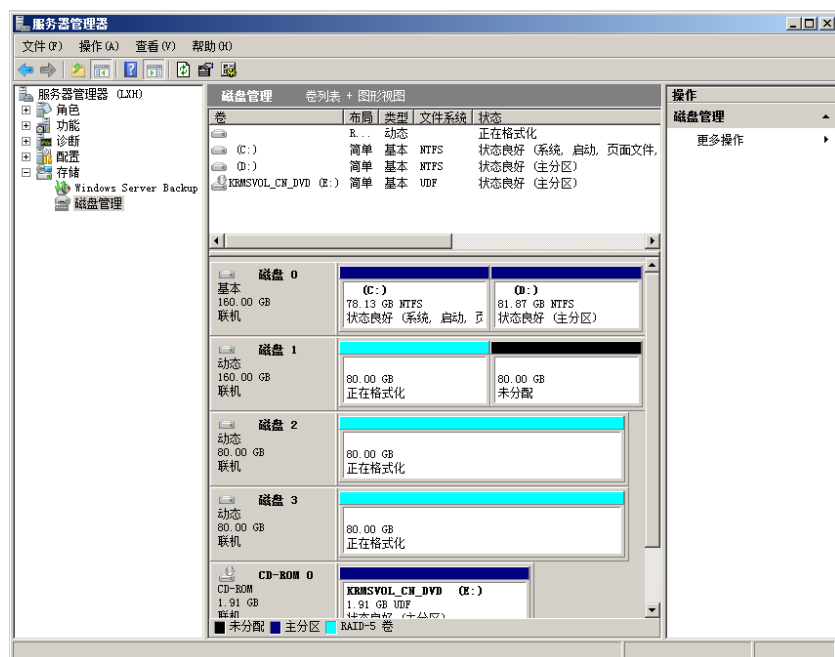


图 10-119 RAID-5 卷创建完成

第 11 章 配置与管理信息共享服务

网站是当前使用最广的信息发布方式，通常是网页制作人员制作相应的网页并上传到 Web 服务器。但对于一些非专业人员，如单位领导或普通用户，如果每次上传网页都要经过专门的技术人员，则不仅效率低下，而且制作的网页可能并不符合自己的意愿。利用微软的 Windows SharePoint Services（以下简称“WSS”）服务可以创建文档信息和共享协助的网站，使用户可以在文档、任务和事件上进行联机协作。并且更容易共享联系人和其他信息，使组和网站管理员更易于管理，从而有助于公司提高员工的工作效率。

11.1 办公自动化系统概述

办公自动化已成为广大企业和公司中不可缺少的部分，一般的办公自动化都是由专业编程人员开发，难以与现有的网站完美集成。而且使用复杂，开发和维护费用都比较高，使得大部分的办公自动化系统的部署仅仅成为“摆设”。WSS 不仅使用简单方便，与 Windows 网站完全兼容。而且可以免费下载，是一种理想的办公自动化系统。

11.1.1 WSS 服务器要求

WSS 服务器的硬件最低和推荐配置如表 11-1 所示。

表 11-1 WSS 服务器的硬件最低和推荐配置

硬件组件	最低配置	推荐配置
CPU	2.5 GHz	3 GHz 双核或更高
内存	1 GB	1 GB
硬盘	至少 3 GB 的可用空间，并且为 NTFS 格式	至少 3 GB 的可用空间，并且为 NTFS 格式
显示设备	支持 1 024x768 的分辨率	支持 1 024x768 的分辨率
网卡	网卡或 Modem	网卡或 Modem

WSS 服务器对软件的要求如下。

（1）为操作系统安装最新补丁程序，以保护系统的安全。在安装 WSS 时，还需要同时安装 IIS 和 Microsoft .NET Framework 3.0 组件。

（2）WSS 服务器应作为域成员服务器，并且服务器场中的成员必须属于同一个域。WSS 也可以安装在独立服务器中（即不加入域），在 DNS 服务器中应设置 WSS 服务器域名。例如，wss.coolpen.net，使其 IP 地址指向 WSS 服务器。

（3）避免将 WSS 网站的用户数据保存在系统分区中，可在其他分区（如 D 和 E 等）中创建一个文件夹，专门用来保存 WSS 网站文件。

11.1.2 解决方案

在 Windows Server 2003 R2 中已经集成了 WSS 服务，版本为 2.0，可以构建企业内部办公站点。在 Windows Server 2008 中并没有集成 WSS，用户需要从微软网站下载 WSS 3.0 SP1 并安装才可搭建 WSS 网站。在配置 WSS 3.0 时，应按照以下步骤执行。

- ① 在服务器中安装 Windows Server 2008 操作系统，将其加入域或者提升为域控制器。
- ② 在 WSS 服务器中安装“Internet 信息服务”，以及 WSS 3.0 SP1 程序。
- ③ 安装完成之后配置 WSS。
- ④ 根据企业要求，创建并配置 Web 网站。

11.2 安装与配置服务器端

在 Windows Server 2008 操作系统中 WSS 功能已经被集成到系统中，用户不需要另行下载即可在 Windows Server 2008 服务器上配置 WSS 服务器，搭建一个功能强大的集成办公网站。

11.2.1 安装前的准备

在安装 WSS 之前，要做好如下准备工作。

- (1) 将计算机加入到域，或者提升为域的辅助域控制器。
- (2) 运行“添加角色向导”，安装 IIS，包括 ASP 和 ASP.NET 组件。
- (3) 运行“添加功能向导”，安装“.NET Framework 3.0”和“SMTP 服务器”，如图 11-1 所示。

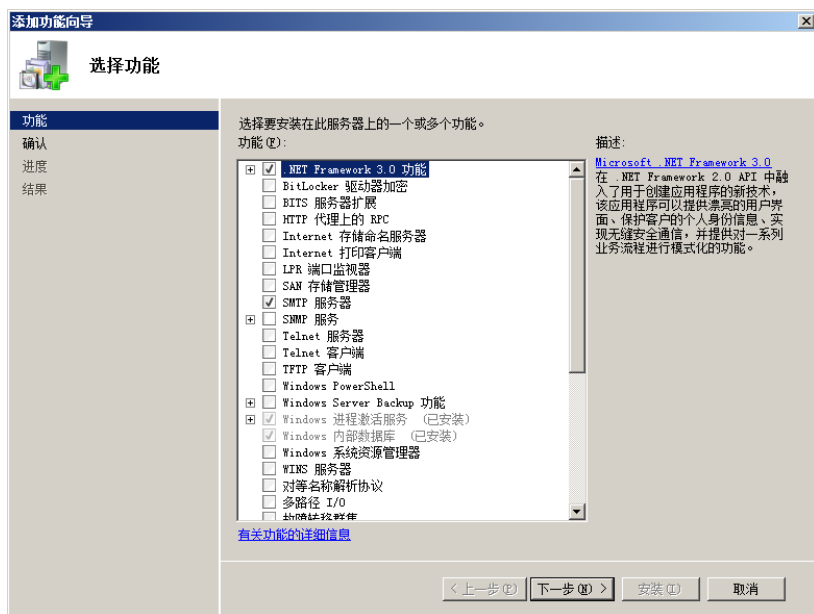


图 11-1 安装“.NET Framework 3.0”和“SMTP 服务器”

11.2.2 安装 WSS

安装 WSS 的操作步骤如下。

- ① 运行已下载 WSS 3.0 安装程序，显示如图 11-2 所示的“阅读 Microsoft 软件许可证条款”对话框，选中“我接受此协议的条款”复选框。
- ② 单击“继续”按钮，显示如图 11-3 所示的“选择所需的安装”对话框，在其中选择安装方式。
- ③ 如果要在独立服务器中安装，则单击“基本”按钮；如果要在域成员服务器中安装，则单击“高级”按钮，显示如图 11-4 所示的“服务器类型”对话框。打开“数据位置”选项卡，指定数据库的安装路径，通常使用默认设置即可。



图 11-2 “阅读 Microsoft 软件许可证条款”对话框



图 11-3 “选择所需的安装”对话框



图 11-4 “服务器类型”对话框

④ 单击“立即安装”按钮，开始安装 WSS，并显示“安装进度”对话框。安装完成后，显示如图 11-5 所示的对话框。默认选中“立即运行 SharePoint 产品和技术配置向导”复选框，在安装完成以后可运行配置向导配置 WSS。



图 11-5 WSS 安装完成对话框

⑤ 单击“关闭”按钮关闭安装向导，并打开如图 11-6 所示的“SharePoint 产品和技术配置向导”对话框，准备配置 WSS。

⑥ 单击“下一步”按钮，显示如图 11-7 所示的提示框，其中列出配置期间可能需要启动或重置的服务。



图 11-6 “SharePoint 产品和技术配置向导”对话框



图 11-7 提示框

⑦ 单击“是”按钮，显示如图 11-8 所示的“正在配置 SharePoint 产品和技术”对话框。开始配置 SharePoint，共有 10 项配置任务。

⑧ 配置完成后显示如图 11-9 所示的“配置成功”对话框。

⑨ 单击“完成”按钮。

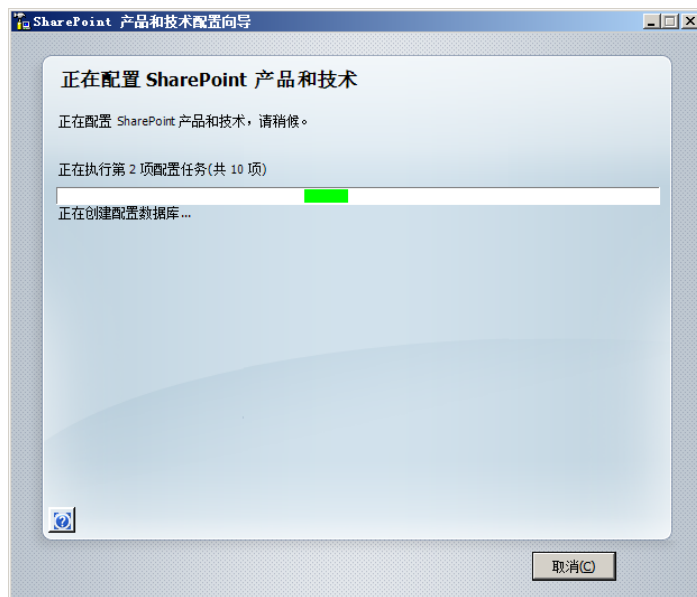


图 11-8 “正在配置 SharePoint 产品和技术”对话框

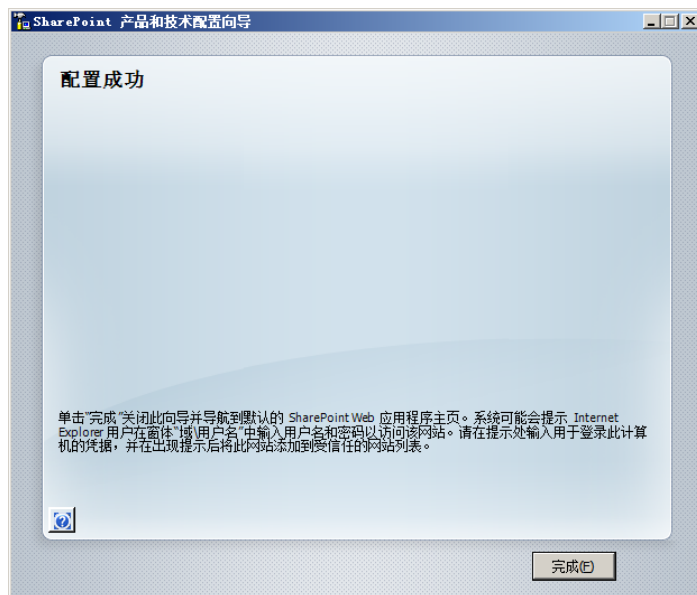


图 11-9 “配置成功”对话框

11.2.3 框架生成与基本功能

WSS 安装完成后会自动连接 WSS 网站主页，首先显示如图 11-10 所示的“连接到”对话框。也可以在 IE 浏览器中输入 WSS 服务器的计算机名或 IP 地址，直接连接 WSS 网站。

提示 默认状态下，只有 Administrator 账户能够登录并访问和管理 WSS 网站，网络管理员可根据需要为不同的用户账户分配不同的权限。

在“用户名”和“密码”文本框中输入管理员用户账户和密码，单击“确定”按钮即可登录到 WSS 网站，如图 11-11 所示。

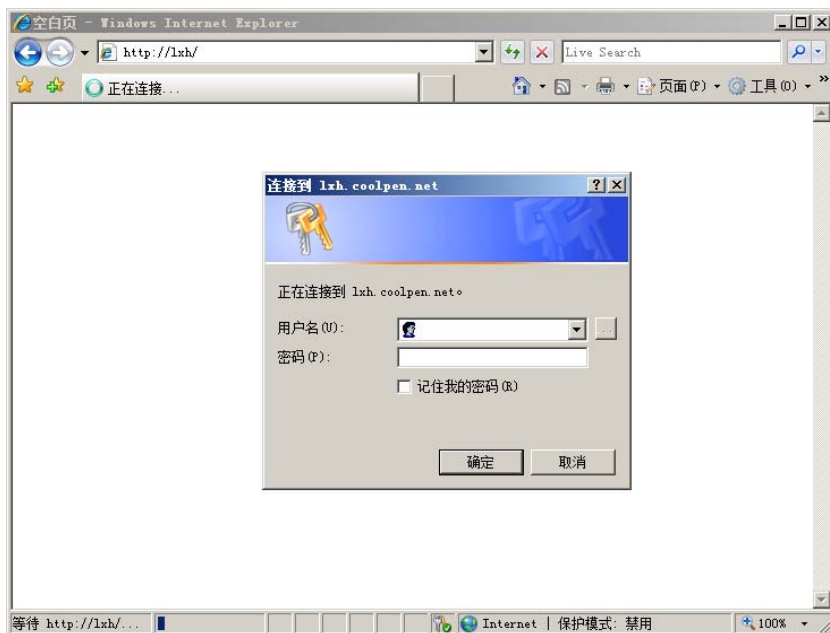


图 11-10 “连接到”对话框

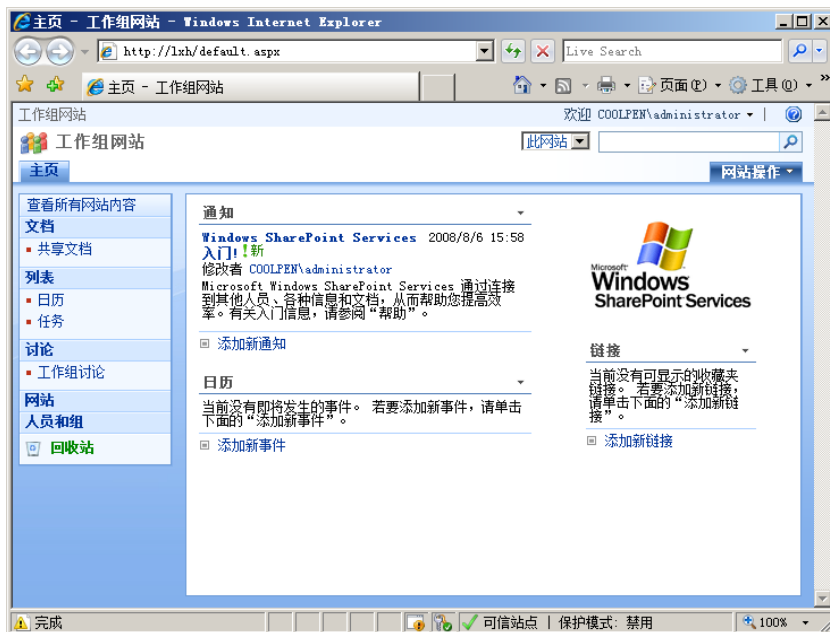


图 11-11 WSS 网站主页

至此用户可以在网络中的任何一台计算机上登录并访问 WSS 网站。

WSS 在刚刚安装完成时，默认只是生成了一个基本框架，没有任何内容。需要网络管理员逐渐完善，如添加通知和事件、上传文档和图片，以及新建讨论、调查和个人网站等，所有这些都可利用 Web 浏览器在 WSS 网站中完成。



提示

默认情况下，只有 Administrator 用户才有访问和管理 WSS 服务器的权限，而其他用户账户都将被拒绝访问，如图 11-12 所示。

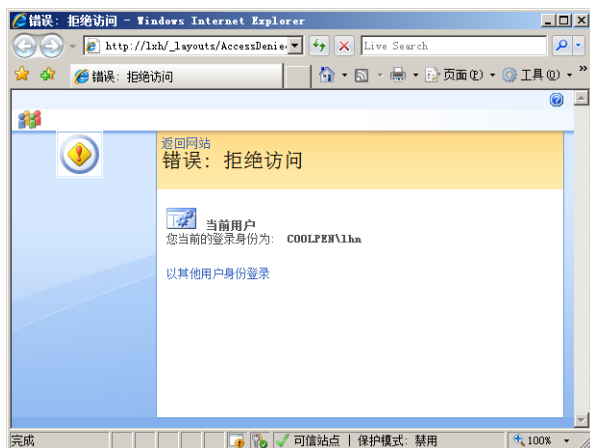


图 11-12 拒绝其他用户访问

11.3 基于 WSS 的办公自动化系统细节设置

WSS 网站具有创建简单及维护方便的特点,可以在其中添加多个用户并分别赋予不同的访问权限。也可以创建一个或多个网站,并分别设置不同的信息或外观,从而满足企业级、部门级及个人使用的要求。

11.3.1 办公自动化站点的用户管理

默认情况下,新创建的 WSS 网站只有 Administrator 账户才能访问和管理。为了允许其他用户访问,应添加其他用户账户,并为不同的用户分配不同的访问权限。用户权限分为以下 4 种。

- (1) 读者: 只有访问权。
- (2) 参与讨论: 可以在文档库和列表中添加内容。
- (3) 设计: 除了“参与讨论”权限外还能创建列表和文档库,以及自定义网页的权限。
- (4) 完全控制: 对网站具有完全的控制权限。

添加用户并为其设置访问权限的操作步骤如下。

① 在 WSS 主页窗口中单击右上角的“网站操作”,在下拉列表框中选择“网站设置”选项,显示如图 11-13 所示的“网站设置”窗口。在其中可以设置“用户和权限”、“外观”、“库”和“网站管理”选项。



图 11-13 “网站设置”窗口

② 单击“人员和组”链接，显示如图 11-14 所示的“人员和组”窗口。默认显示“工作组网站成员”窗口，并且没有任何用户。在其中添加的账户将具有参与 SharePoint 网站讨论的权限，在左侧的“组”栏中可以为网站设置 3 种用户组，分别具有如下权限。

工作组网站成员：该组的成员将具有参与 SharePoint 网站讨论的权限，默认没有任何用户。

工作组网站访问者：该组的成员具有读取 SharePoint 网站的权限，即仅有浏览权限，默认没有任何用户。

工作组网站所有者：该组的成员具有对 SharePoint 网站的完全控制权限，默认只有 Administrator 用户。



图 11-14 “人员和组：工作组网站成员”窗口

③ 以设置“工作组网站成员”为例，单击“新建”按钮，显示如图 11-15 所示的“添加用户”窗口。在“用户/用户组”文本框中键入要添加的用户或组，如果是域用户或组，应使用“域\用户或组”的格式；如果是本地服务器的用户或组，则直接键入相应名称。在“授予权限”选项组中默认选择“向 SharePoint 用户组添加用户”单选按钮，为用户分配“参与讨论”权限。也可以选择“直接授予用户权限”单选按钮，直接为用户分配权限。当输入多个用户或组时，需用分号隔开。

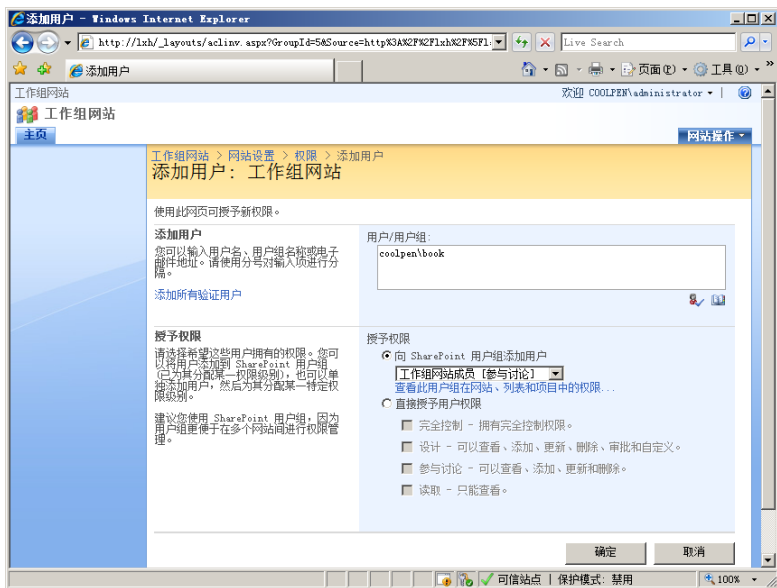


图 11-15 “添加用户”窗口

④ 单击“确定”按钮，添加完成的用户组如图 11-16 所示。该组的用户具有参与 WSS 网站讨论的权限，执行同样操作可添加多个用户。



图 11-16 添加完成的用户

通常情况下，对于企业员工及网站的普通访问者，可以授予“读者”或“讨论参与者”权限；对于部门的网站管理者，可以授予“网站设计者”的权限；“完全控制”权限则应为管理员所拥有，以保护 WSS 网站的安全。

11.3.2 管理网站和工作区

在“网站和工作区”页面中可以创建个人网站、文档工作区及会议工作区。

① 打开“网站设置”窗口，单击“网站和工作区”链接，显示如图 11-17 所示的“网站和工作区”窗口。

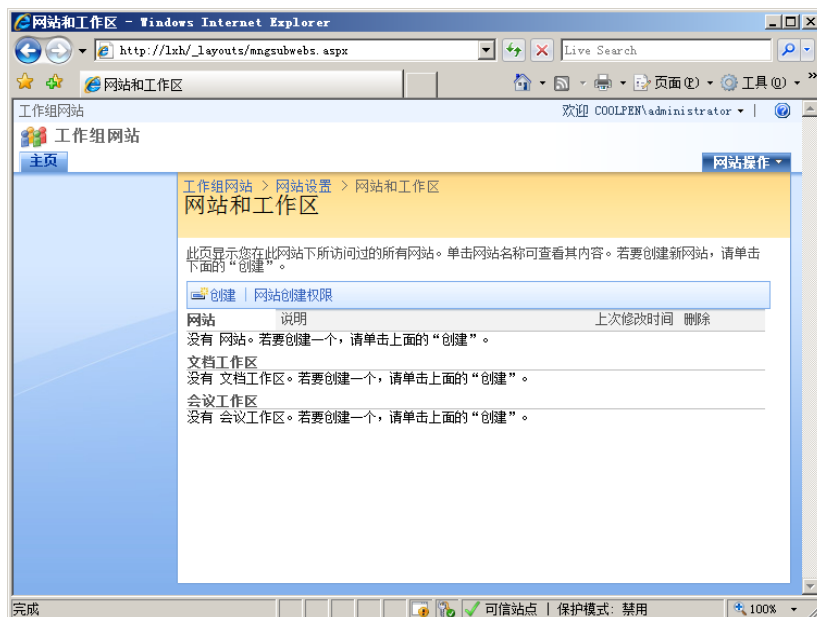


图 11-17 “网站和工作区”窗口

② 单击“创建”按钮，显示如图 11-18 所示的“新建 SharePoint 网站”窗口。在“标题”和“说明”文本框中键入新 SharePoint 网站的标题和说明；在“URL 名称”文本框中为新网站定义一个地址，用于其他用户的访问；在“选择模板”列表框中为新网站选择一个模板；在“用户权限”选项区域中为该网站选择权限，可以使用与父网站相同的权限，也可以使用独立权限。



图 11-18 “新建 SharePoint 网站”窗口

③ 单击“创建”按钮，创建完成一个新的 SharePoint 网站，如图 11-19 所示。

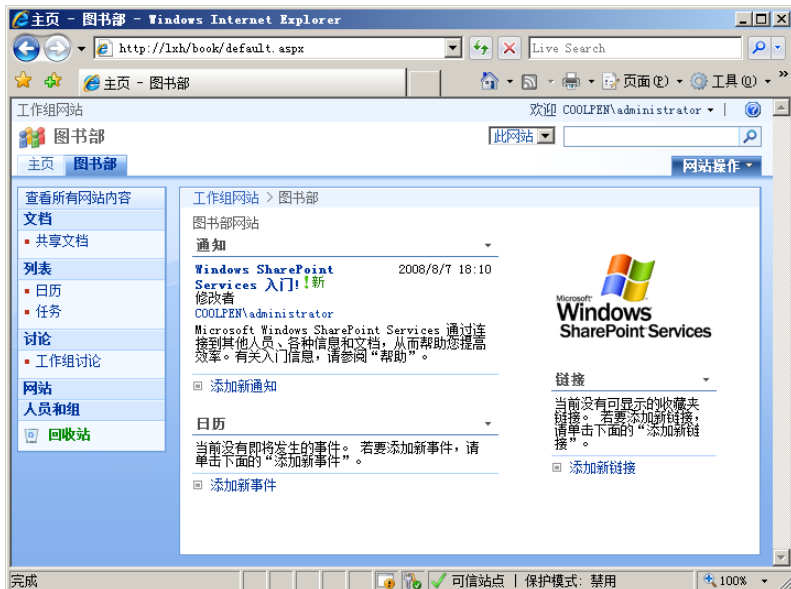


图 11-19 创建完成一个新的 SharePoint 网站

至此，个人网站创建完成，用户使用其 URL 地址即可访问该网站。

11.3.3 配置网站和创建工作区

创建完成个人网站以后，还可以为其分配权限。不过只能分配“设计”和“参与讨论”两种权限。

① 返回 WSS 网站主页，打开“网站和工作区”窗口。单击“网站创建权限”按钮，显示如图 11-20 所示的“网站和工作组创建”窗口，为网站和工作区选择权限级别。

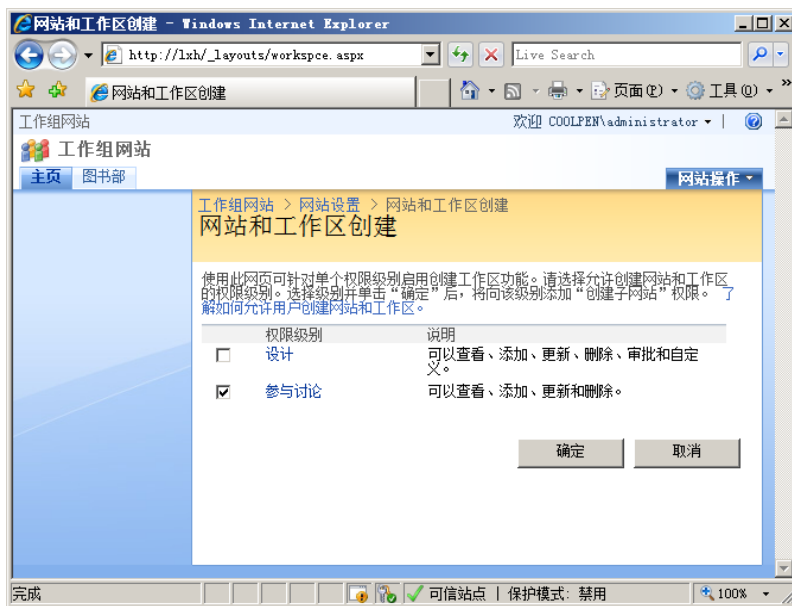


图 11-20 “网站和工作组创建”窗口

② 单击“确定”按钮保存设置。

11.3.4 更改网站标题和说明

WSS 网站的主页标题默认为“工作组网站”，可以将其更改为能够彰显公司个性的标题及徽标。同样，已创建的个人网站也可以更改标题和说明。

① 打开“网站设置”窗口，单击“外观”选项选组中的“标题、说明和图标”超级链接，显示如图 11-21 所示的“标题、说明和图标”窗口。在“标题”和“说明”文本框中分别键入网站的标题和说明；在“URL”文本框中键入作为网站徽标的图片文件链接地址，可使用绝对路径（例如 <http://www.coolpen.net/logo.gif>），也可以使用相对路径（例如 [image/logo.gif](#)）。

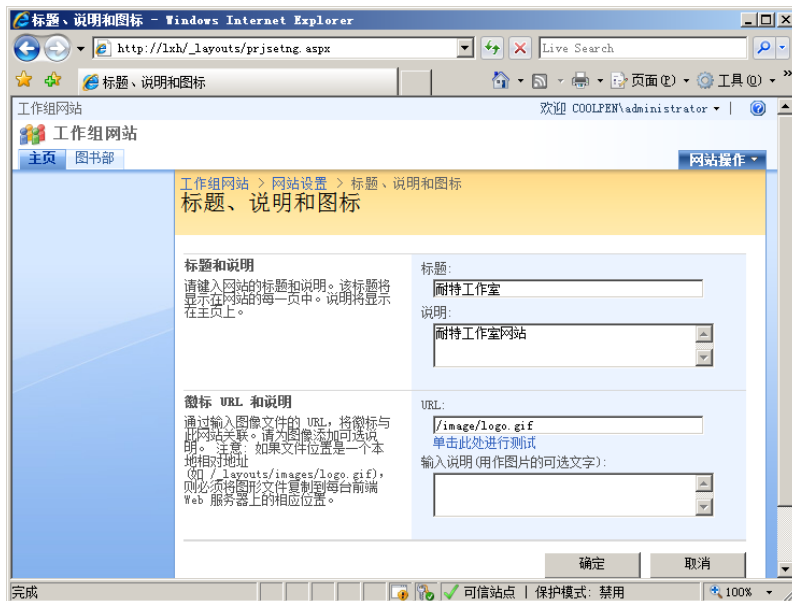


图 11-21 “标题、说明和图标”窗口

- ② 单击“确定”按钮保存网站设置。

11.3.5 修改网站主题

与 Windows 外观主题一样，WSS 网站也可以使用醒目的主题，并且 WSS 内置了十几种主题可供选择。不过网站主题只是更改网站的字体和配色方案，并不会影响网站的布局，也不会更改已单独应用主题的网页。

- ① 在“网站设置”窗口中单击“外观”选项组中的“网站主题”超级链接，显示如图 11-22 所示的“网站主题”窗口。在主题列表中可选择主题，同时在左侧“预览”区域中显示预览图像。

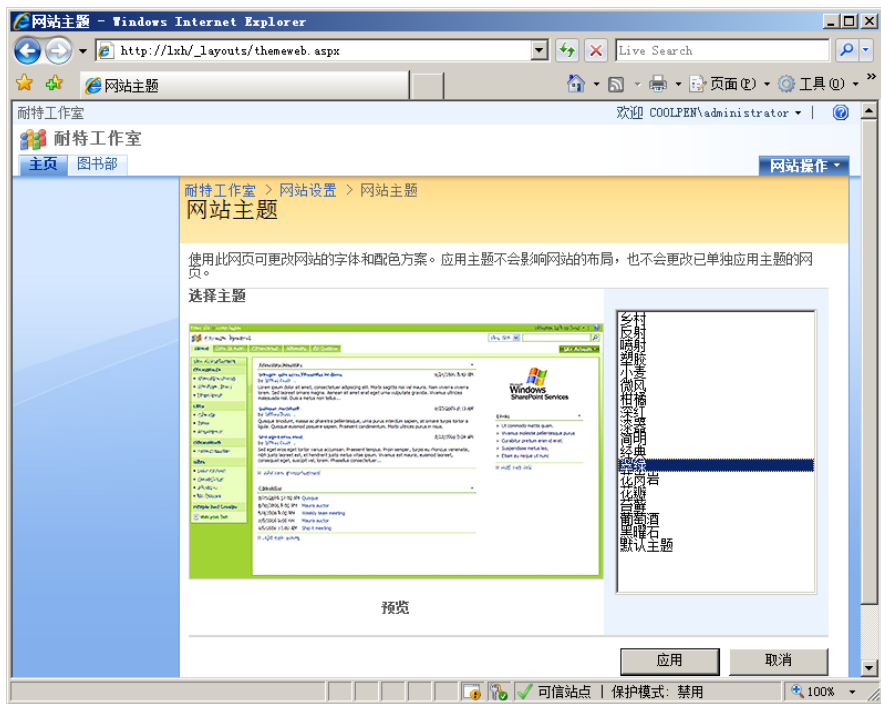


图 11-22 “网站主题”窗口

- ② 单击“应用”按钮，即可应用已选择的主题，已创建的个人网站也可以选择使用不同的主题。

11.3.6 自定义主页

默认状态下，WSS 已经创建网页。并且网页中的各种部件都采用模块化，可以随意修改。如果用户对网页的布局不满意，可以编辑。不需使用专门的制作软件，只需添加、删除或者移动相应的部件即可制作自己喜欢的网页。

- ① 在 WSS 网站主页中单击“网站操作”按钮，显示如图 11-23 所示的编辑网页窗口，此时所有的部件都可以删除或者更改位置。

- ② 如果要在左栏中添加一个 Web 部件，单击左栏中的“添加 Web 部件”按钮。显示如图 11-24 所示的“向左栏添加 Web 部件”对话框，在列表框中选择要添加的部件即可。

- ③ 单击“添加”按钮，所选择的部件将添加到 WSS 网页中。执行同样操作，也可以在右栏中添加部件，完成后的网页如图 11-25 所示。

- ④ 网页设计完成以后，单击右上角的“退出编辑模式”链接退出编辑模式，网页自定义完成。

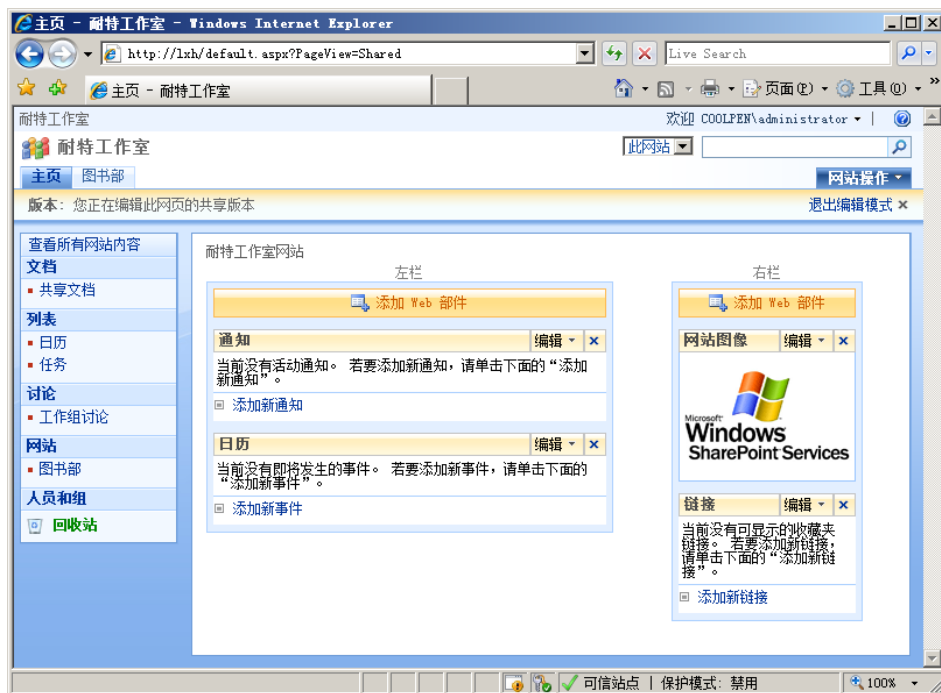


图 11-23 编辑网页窗口



图 11-24 “向左栏添加 Web 部件”对话框

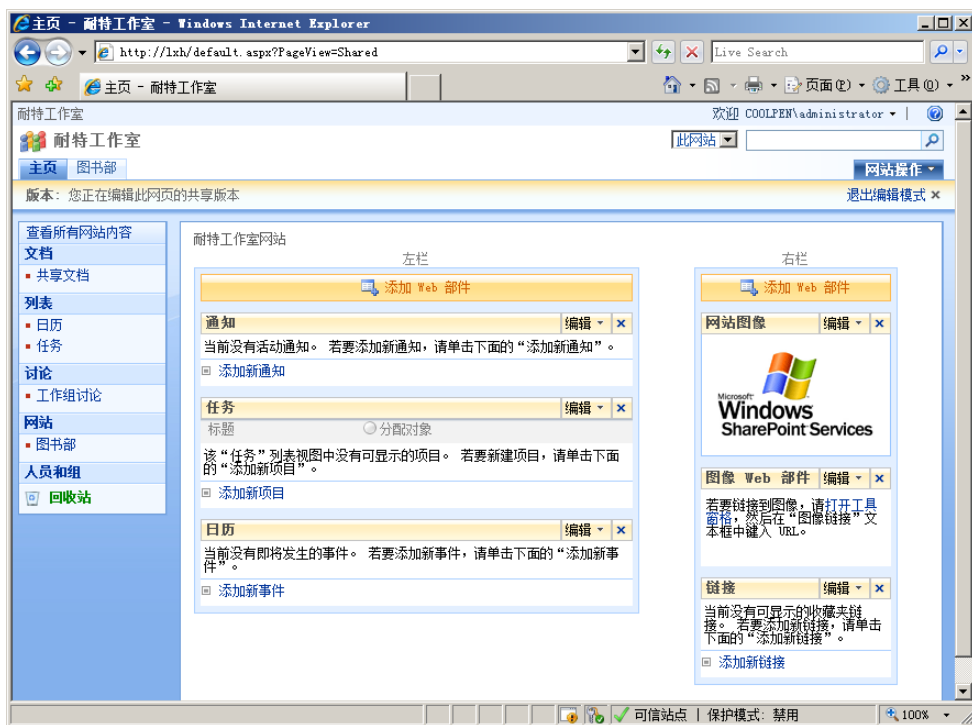


图 11-25 完成后的网页

11.3.7 修改当前登录用户信息

在 WSS 站点中, 用户的信息从 Active Directory 数据库中读取, 在 WSS 网页上也只是显示用户名。例如, 刘晓辉的用户名是“liuxh”, 则在 WSS 网页上显示的也是 liuxh。为了美观和易于查看, 可以设置为在 WSS 网页上用户的中文名称或者指定其他名称。需要注意的是, 只有使用具有完全控制权限的账户登录后才能更改用户名称。

① 打开“网站设置”窗口, 单击“用户和权限”选项组中的“人员和组”超级链接, 打开“人员和组”窗口。在左侧栏中单击“所有人员”选项, 显示如图 11-26 所示的“人员和组: 所有人员”窗口, 其中列出在 WSS 中已添加的所有用户。

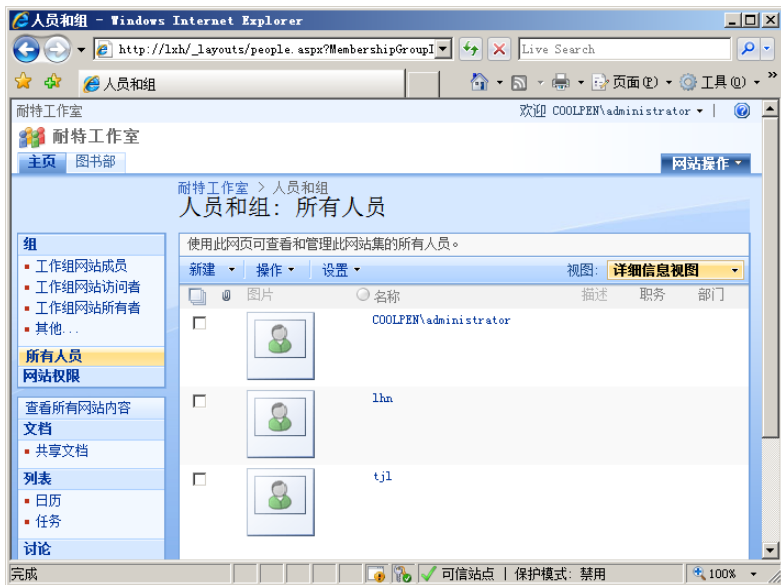


图 11-26 “人员和组: 所有人员”窗口

② 单击要更改显示名称的用户，显示如图 11-27 所示的“用户信息”窗口，其中列出该用户的所有信息。



图 11-27 用户信息

③ 单击“编辑项目”按钮，显示如图 11-28 所示的“编辑个人设置”窗口。在“名称”文本框中键入该用户的显示名称，在“电子邮件”文本框中键入该用户的电子邮件地址。

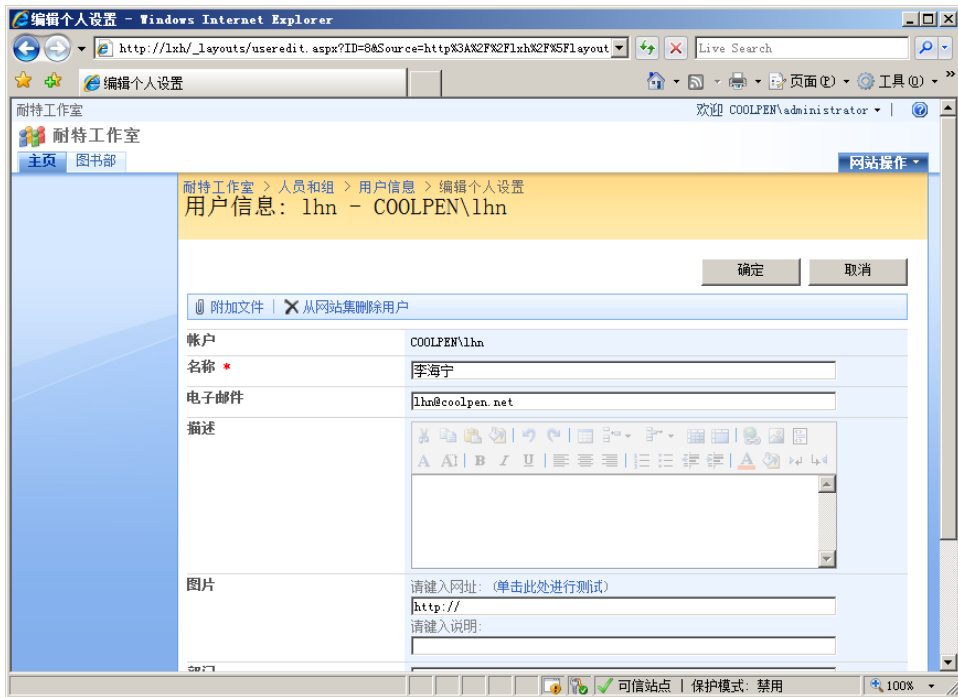


图 11-28 “编辑个人设置”窗口

④ 单击“确定”按钮，保存设置。然后在 WSS 网站中单击右上角的用户名，选择下拉菜单中的“以其他用户身份登录”选项，使用已更改名称的用户账户登录。显示更改的名称，如图 11-29 所示。

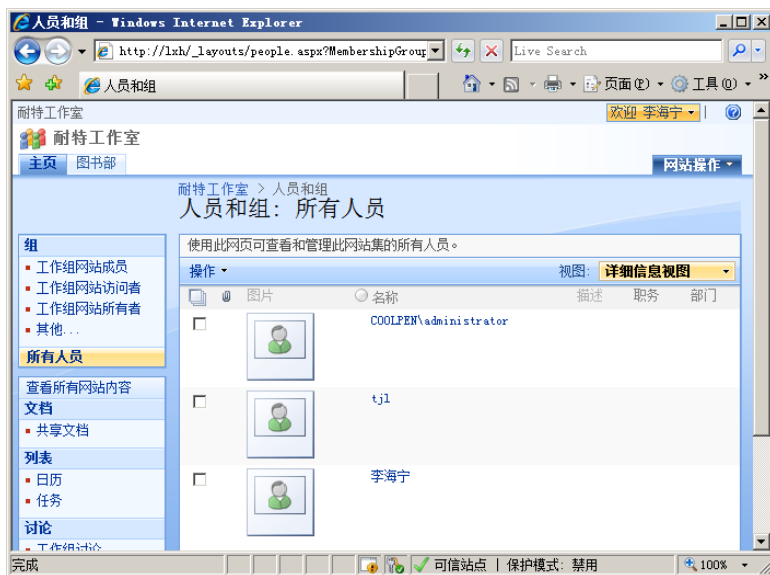


图 11-29 更改的名称

11.3.8 修改当前用户的通知

通知可将网站上的任何内容更改通过电子邮件告知各用户，也可以为列表和库及其中各项创建通知。为列表或库创建通知时，可指定希望跟踪的更改类型。例如，可设置为在添加、修改、删除项目或文件时收到服务器通知，也可设置为在更新、删除文件或项目时收到文件和列表项目通知。对于库中文档，可设置为在添加、删除或编辑 Web 讨论中的评论时收到通知。

① 登录到 WSS 网站以后，单击右上角的用户名。选择下拉列表框中的“我的设置”选项，显示如图 11-30 所示的“个人设置”窗口。



图 11-30 “个人设置”窗口

② 单击“我的通知”按钮，显示如图 11-31 所示的“我的有关此网站的通知”窗口，其中显示所有添加的通知。

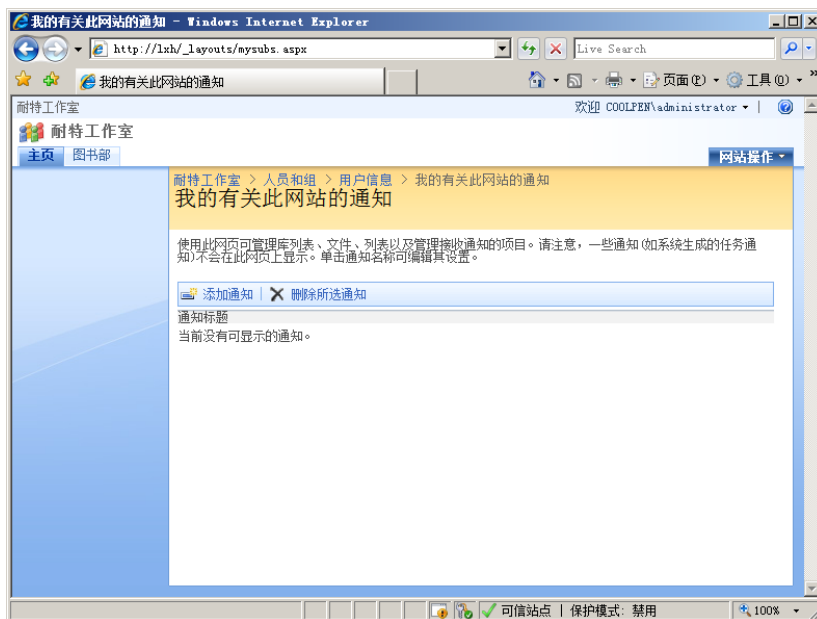


图 11-31 “我的有关此网站的通知”窗口

③ 单击“添加通知”按钮，显示如图 11-32 所示的“新建通知”窗口，选择“通知”单选按钮。



图 11-32 “新建通知”窗口

④ 单击“下一步”按钮，显示如图 11-33 所示的“新建通知”窗口。在“通知标题”文本框中键入通知的标题；在“通知发送对象”文本框中键入接收此通知的用户名，多个用户以分号隔开；在“更改类型”选项组中指定哪些更改发生时发送通知；在“针对这些更改发送通知”选项组中根据条件筛选通知；在“发送通知的时间”选项组中指定通知的发送频率。

⑤ 单击“确定”按钮，添加完成通知。



图 11-33 “新建通知”窗口

11.3.9 查看网站用户的信息

在“网站设置”窗口中单击“人员和组”超级链接，打开“人员和组”窗口。单击左侧栏中的“所有人员”按钮，显示 WSS 网站中的所有用户，如图 11-34 所示。如果要查看用户所具有的权限，可在左侧栏的“组”列表中选择。



图 11-34 查看用户

11.4 WSS 网站管理

WSS 网站管理主要用来管理用户和 SharePoint 用户组的权限，为了使不同的用户在访问 WSS 网站时能够执行不同的操作，需要通过为不同用户和 SharePoint 组赋予不同的权限来实现。

11.4.1 管理用户和权限

管理用户和权限包括人员和组、网站集管理员和高级权限 3 个部分。

1. 管理用户和人员

在“网站设置”窗口中单击“用户和权限”选项组中的“人员和组”超级链接，显示如图 11-35 所示的“人员和组”窗口。在其中可管理用户和组，包括添加和删除用户，以及设置权限等，操作方法请参见前面所述内容。

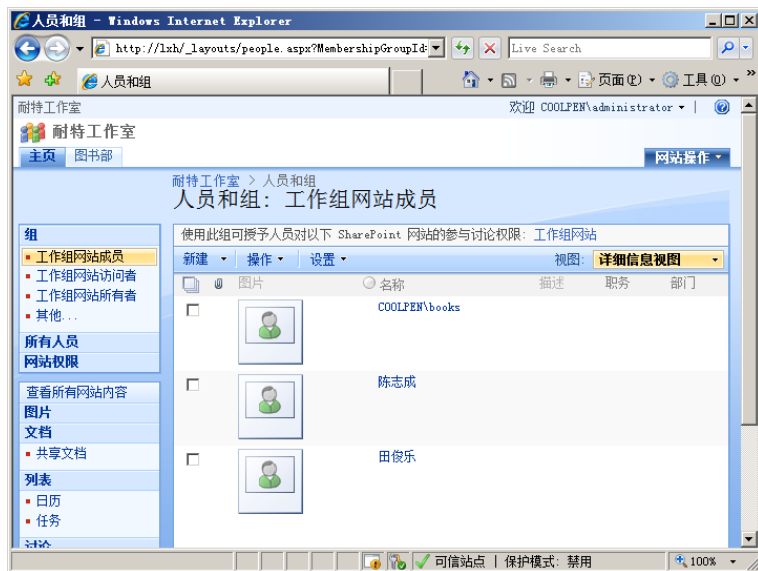


图 11-35 “人员和组”窗口

2. 添加网站集管理员

默认状态下，在 WSS 网站中只有 Administrator 用户才具有访问和管理权限，并且对所有网站都拥有完全控制权限。如果需为某个特定用户也赋予这种权限，可以通过添加“网站集管理员”的方式来实现。

在“网站设置”窗口中，单击“用户和权限”选项组中的“网站集管理员”超级链接，显示如图 11-36 所示的“网站集管理员”窗口。在文本框中添加网站集管理员，多个用户之间要用分号分隔。



图 11-36 “网站集管理员”窗口

单击“确定”按钮，为新用户赋予完全控制权限。需要注意的是，添加网站集管理员时只能添加单个用户，不能添加用户组。

3. 高级权限

默认状态下，WSS 网站只有 3 个 SharePoint 组，即工作组网站成员、工作组网站访问者和工作组网站所有者，分别具有参与讨论、读取和完全控制权限。网站管理员也可以更改 SharePoint 组的权限，或者添加 SharePoint 组。

① 在“网站设置”窗口中单击“用户和权限”选项组中的“高级权限”超级链接。显示如图 11-37 所示的“权限”窗口，其中默认显示系统内置的 3 个 SharePoint 组。



图 11-37 “权限”窗口

② 如果要更改某个用户组的权限，则单击 SharePoint 组名，显示如图 11-38 所示的“编辑权限”窗口。在“权限”选项组中选择要赋予的权限即可，单击“确定”按钮保存设置。



图 11-38 “编辑权限”窗口

③ 如果要添加新的 SharePoint 组，则在“权限”窗口中单击“新建”按钮右侧的黑色箭头。在下拉菜单中选择“新建用户组”选项，显示如图 11-39 所示的“新建用户组”窗口。在“名称”文本框中键入新组的名称，在“用户组所有者”文本框中键入该组的所有者用户，在“授予用户组对此网站的权限”选项组中选择要授予该组的权限。

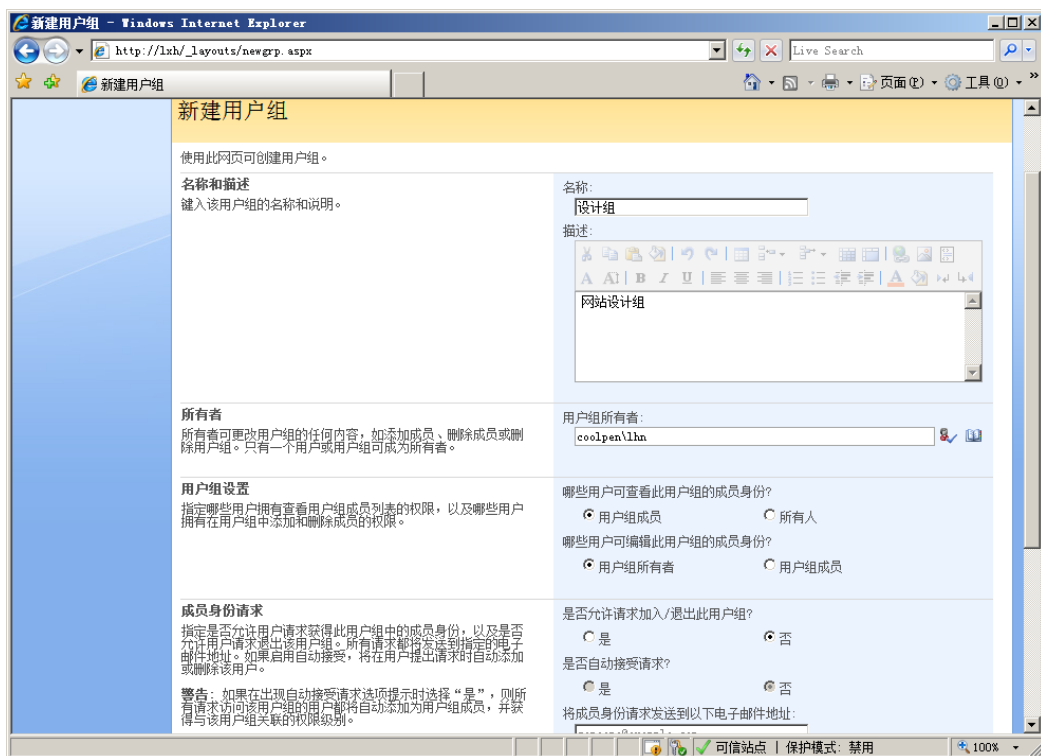


图 11-39 “新建用户组”窗口

④ 单击“创建”按钮，创建完成一个新的用户组，如图 11-40 所示。



图 11-40 已创建的一个新用户组

11.4.2 网站管理

1. 将网站另存为模板

WSS 提供了一个“导入/导出”功能，当网站管理员将 WSS 网站的整体框架配置完成之后，即将

其保存成一个模板。以后如果需要创建类似的网站时，只需导入此模板。

① 在“网站设置”窗口中单击“外观”选项组中的“将网站另存为模板”超级链接，显示如图 11-41 所示的“将网站另存为模板”窗口。在“文件名”文本框中键入模板文件名，在“模板名称”文本框中键入该模板的名称。



图 11-41 “将网站另存为模板”窗口

② 单击“确定”按钮，即可将网站成功保存为模板，并显示如图 11-42 所示的“操作成功完成”窗口。

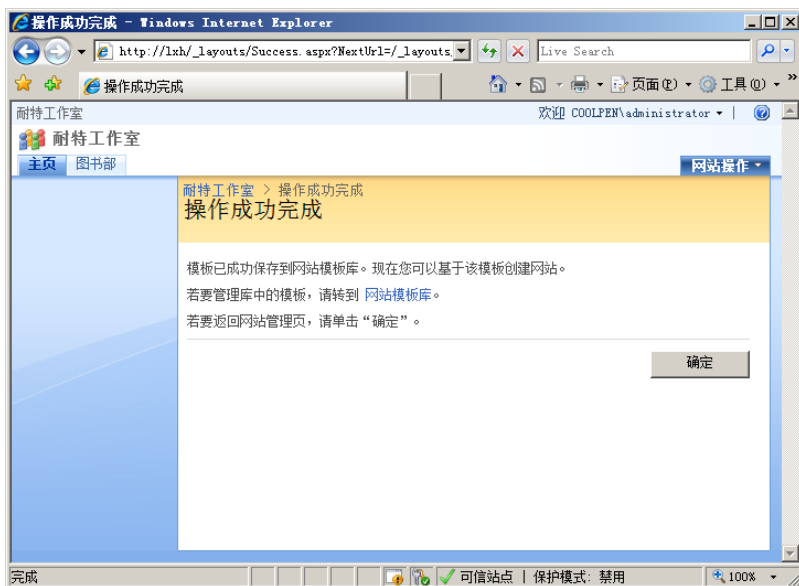


图 11-42 “操作成功完成”窗口

2. 区域设置

在“网站设置”窗口中单击“网站管理”选项组中的“区域设置”超级链接，显示如图 11-43 所示的“区域设置”窗口，在其中设置 WSS 网站的区域、排序方式、时区、日历及工作周等。

3. 网站库和列表

(1) 在“网站设置”窗口中，单击“网站管理”选项组中的“网站库和列表”超级链接，显示如

图 11-44 所示的“网站库和列表”窗口，在其中更改列表、文档库、讨论版或调查的设置。

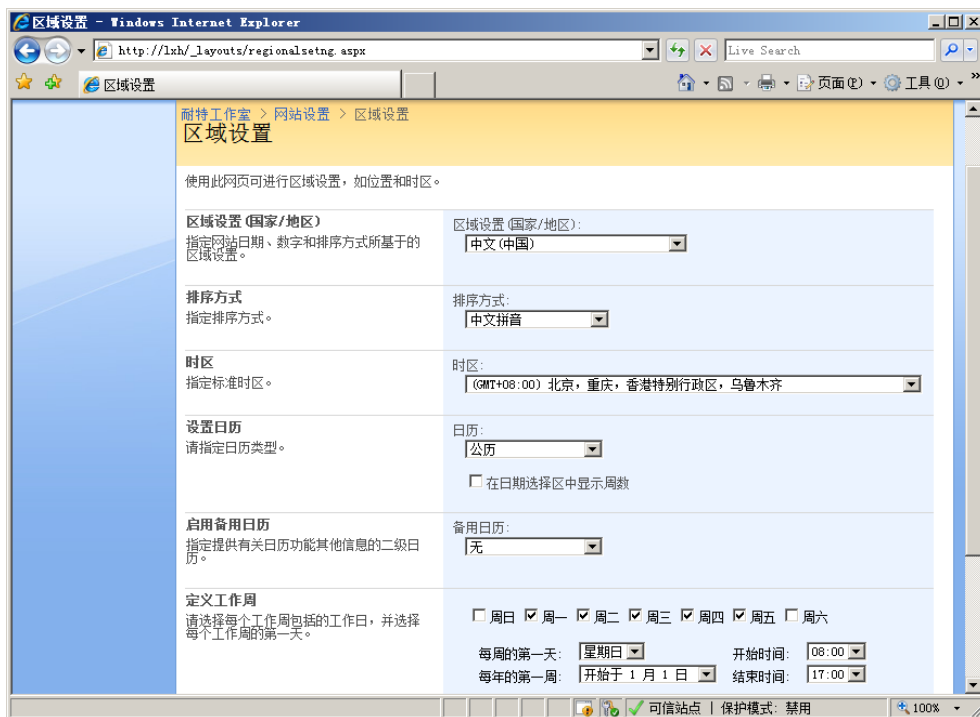


图 11-43 “区域设置”窗口

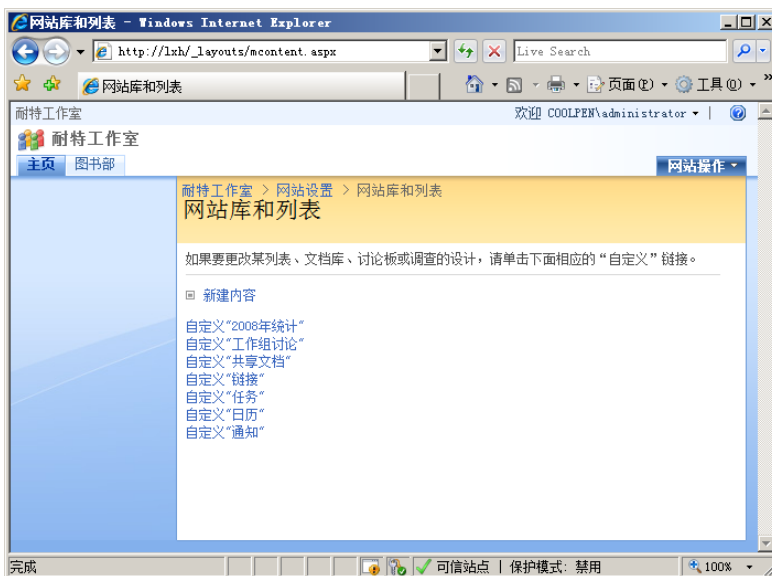


图 11-44 “网站库和列表”窗口

(2) 以更改“共享文档”为例，单击“自定义‘共享文档’”超级链接，显示如图 11-45 所示的“自定义共享文档”窗口。在其中更改共享文档的各种设置，包括常规、权限及视图等。

4. 用户通知

在“网站设置”窗口中单击“网站管理”选项组中的“用户通知”超级链接，显示如图 11-46 所示的“用户通知”窗口。在其中可以管理用户通知，单击“更新”按钮，可以更新网站中的用户通知；单击“删除所选通知”按钮，可删除用户通知。



图 11-45 “自定义共享文档”窗口



图 11-46 “用户通知”窗口

5. 网站和工作区

在“网站设置”窗口中单击“网站管理”选项组中的“网站和工作区”超级链接，显示如图 11-47 所示的“网站和工作区”窗口，其中显示 WSS 网站中所有的网站及工作区。

如果要查看网站或工作区内容，单击相应的网站或工作区名称即可；如果要删除某个工作区，则单击相应的“删除”按钮，显示如图 11-48 所示的“删除此网站”窗口，单击“删除”按钮即可删除工作区。

6. 删除网站

如果要删除当前的 WSS 网站，则在“网站设置”窗口中单击“网站管理”选项组中的“删除此网站”超级链接，显示如图 11-49 所示的“删除此网站”窗口。单击“删除”按钮，将删除整个网站，包括文档、事件、通知及讨论等设置，因此应慎用此项功能。

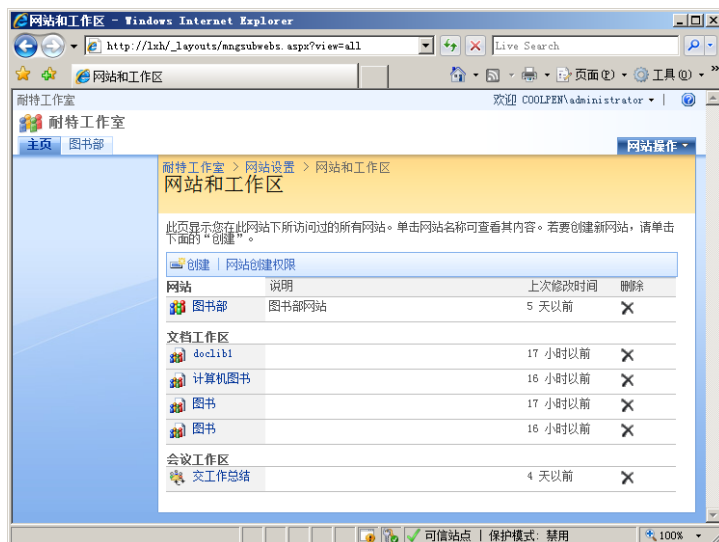


图 11-47 “网站和工作区”窗口

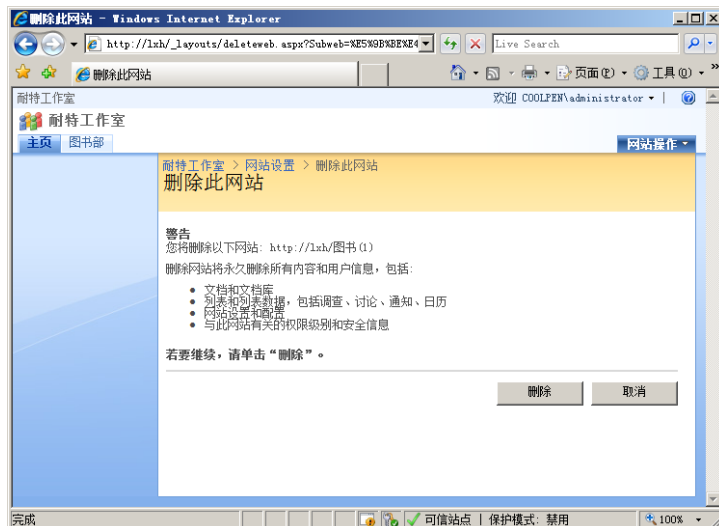


图 11-48 “删除此网站”窗口

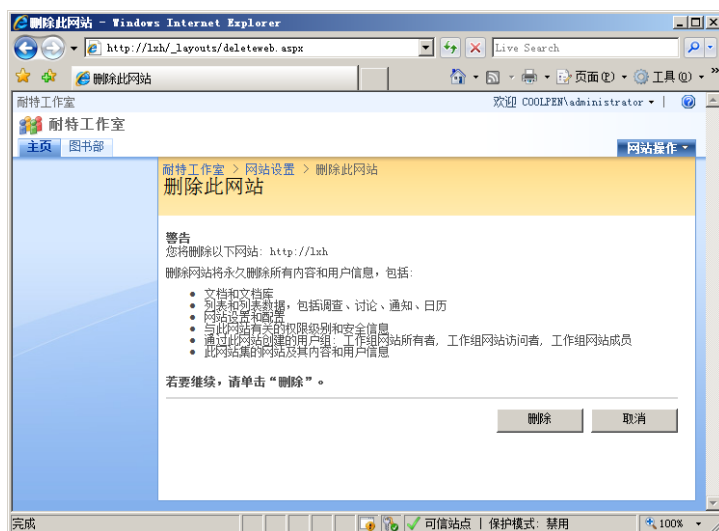


图 11-49 “删除此网站”窗口

11.4.3 网站集管理

1. 回收站

WSS 具有“回收站”功能，和 Windows 系统中的回收站类似。在 WSS 网站中删除某个网站或工作区时，默认并不是从网站中彻底删除，而是删除到回收站中。用户还可以从回收站中回收，以防误删。

在“网站设置”窗口中单击“网站集管理”选项组中的“回收站”超级链接，显示如图 11-50 所示的“网站集回收站”窗口，其中列出了所有曾经删除的项目。

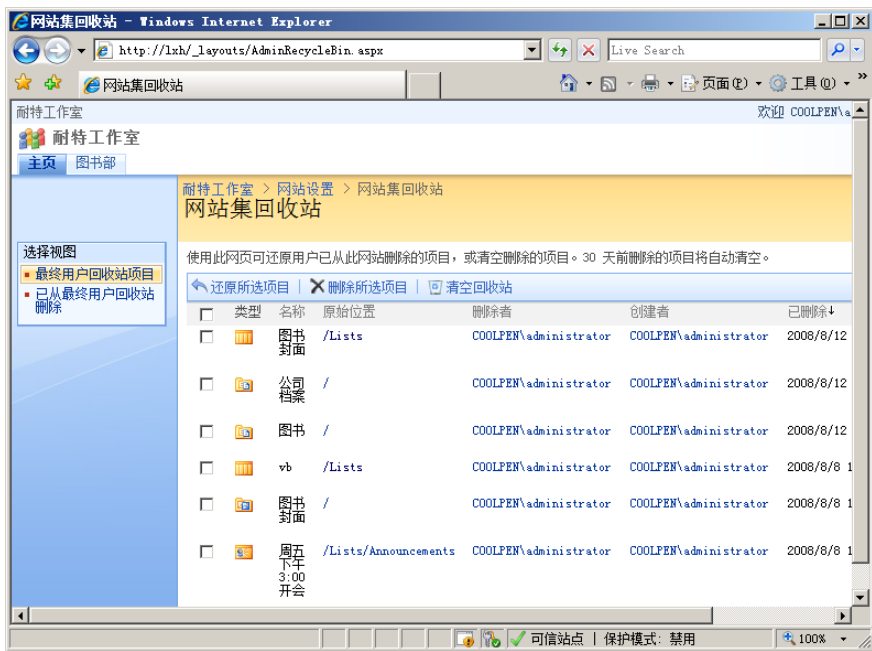


图 11-50 “网站集回收站”窗口

如果要还原某个项目，选中相应的复选框。单击“还原所选项目”按钮，显示如图 11-51 所示的提示框，单击“确定”按钮即可还原。

如果要彻底删除某个项目，选中相应的复选框。单击“删除所选项目”按钮，显示如图 11-52 所示的提示框，单击“确定”按钮即可将其从回收站中彻底删除。



图 11-51 提示框



图 11-52 提示框

2. 网站层次结构

(1) 在“网站设置”窗口中单击“网站集管理”选项组中的“网站层次结构”超级链接，显示如图 11-53 所示的“网站层次结构”窗口。其中显示所有在 WSS 根网站下创建的网站，单击网站名称，即可查看其内容。

(2) 如果要管理某个网站，则单击该网站右侧的“管理”超级链接。显示如图 11-54 所示的“网站设置”窗口，在其中可以实现管理该网站的所有功能。

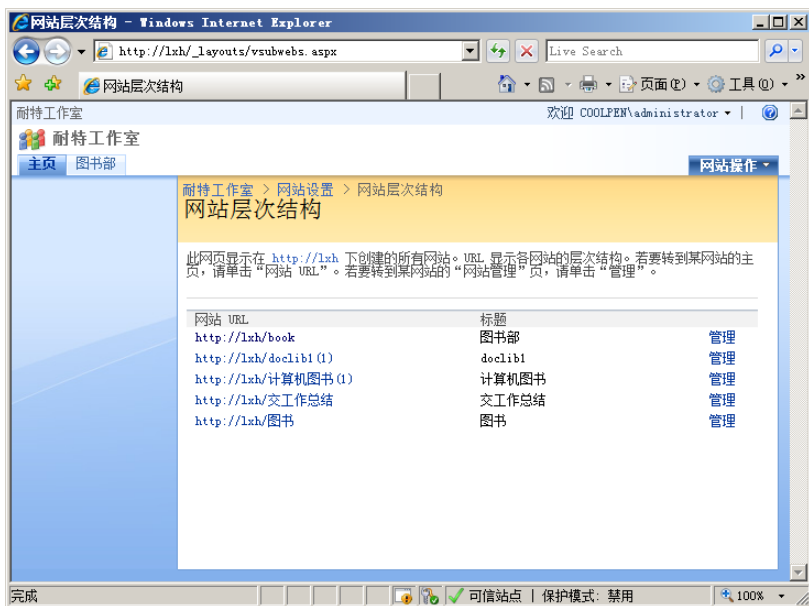


图 11-53 “网站层次结构”窗口



图 11-54 “网站设置”窗口

3. 门户网站连接

如果配置“门户网站连接”，可以将用户的网站连接到与 WSS 兼容的门户网站，使用户能够操作分类网站中的列表（例如通知及事件列表等）、连接到用户配置文件（其中保存用户的基本信息）、连接到门户搜索服务和处理其他信息。

在“网站设置”窗口中单击“网站集管理”选项组中的“门户网站连接”超级链接，显示如图 11-55 所示的“门户网站连接”窗口，默认不连接到门户网站。

如果要连接到门户网站，则选择“连接到门户网站”单选按钮。在“门户网址”文本框中输入门户网站的地址，在“门户网站名称”文本框中输入门户网站的名称，单击“确定”按钮。

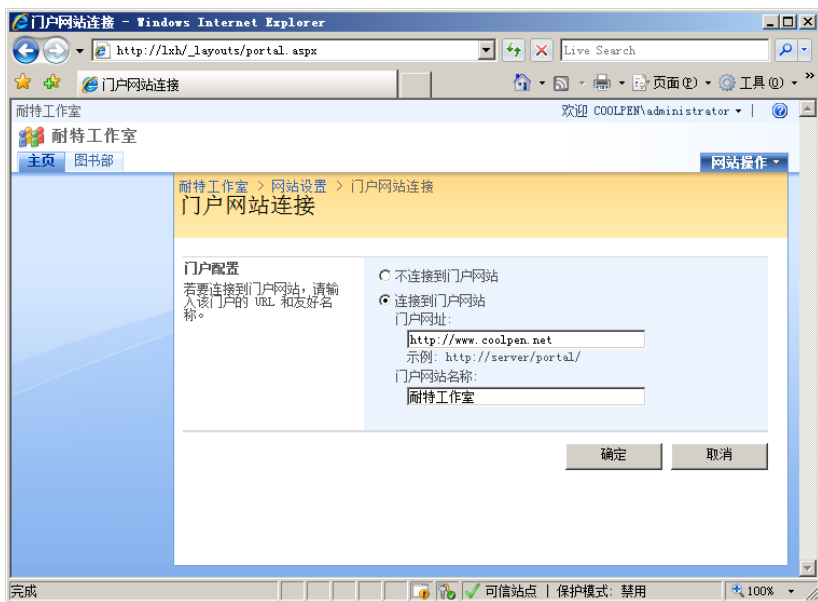


图 11-55 “门户网站连接”窗口

11.5 通知管理

在 WSS 网站中可以轻松地向网站发布通知等信息，并且不需要专业网页制作技术。即使用户对网页制作一窍不通，也可以利用通知功能在很短的时间内发布一封专业的通知，当他人浏览该网站时即可看到。

11.5.1 添加通知

添加通知的操作步骤如下。

① 登录到 WSS 主页，单击“通知”超级链接，显示如图 11-56 所示的“通知”窗口，其中显示所有添加的通知。

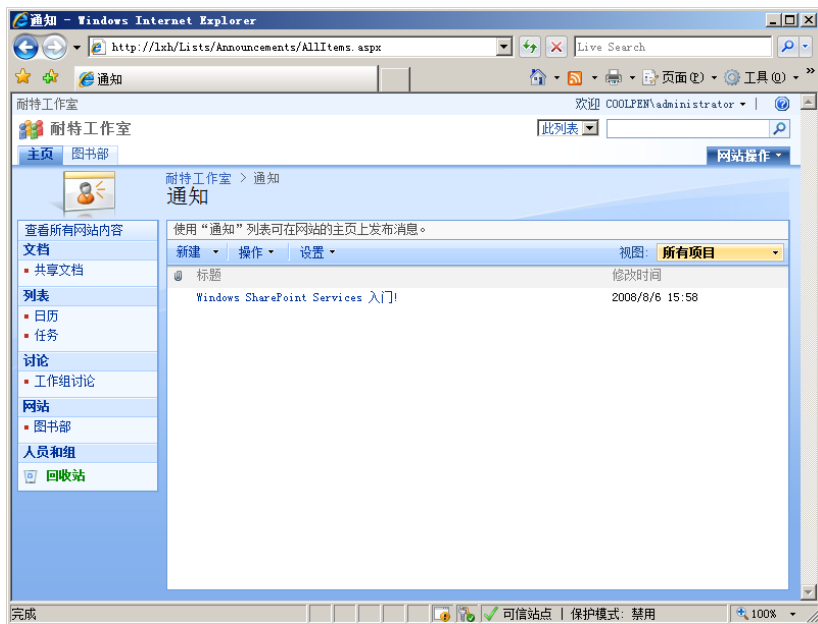


图 11-56 “通知”窗口

② 单击“新建”按钮，或者在 WSS 主页中单击“通知”选项组的“添加新通知”超级链接，显示如图 11-57 所示的“通知：新建项目”窗口。在“标题”文本框中输入新通知的名称；在“正文”文本框中输入通知的内容；在“到期日期”文本框中输入通知的到期日期，到了“到期日期”以后，该通知就会自动删除。

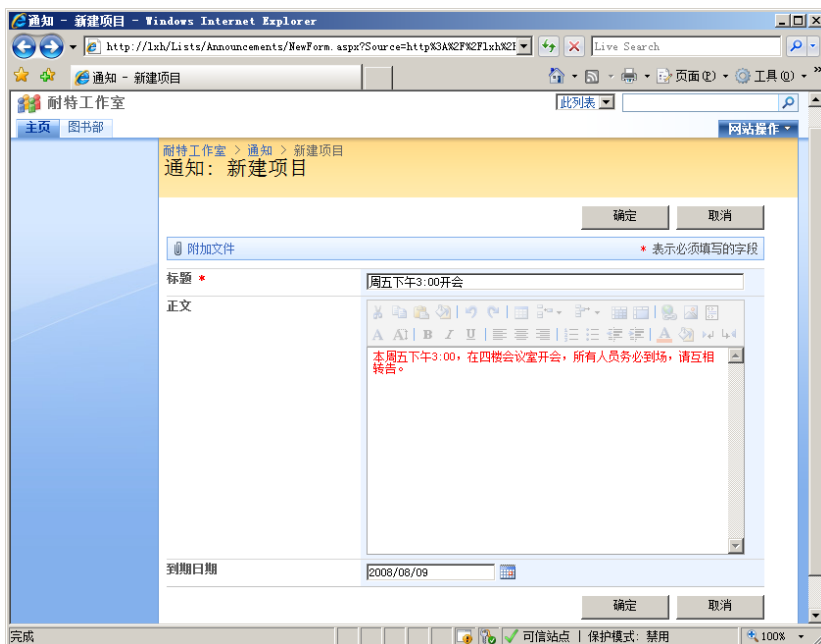


图 11-57 “通知：新建项目”窗口

③ 单击“确定”按钮，一条通知添加完成。并显示在 WSS 主页的“通知”选项组中，如图 11-58 所示。



图 11-58 新的通知

按照同样操作步骤，可继续添加其他通知。

11.5.2 编辑通知

如果发布通知以后，发现其中的内容有误，或者需要进一步修改，则可以重新编辑通知。

- ① 在“通知”窗口中单击待修改的通知，显示如图 11-59 所示的通知的属性。

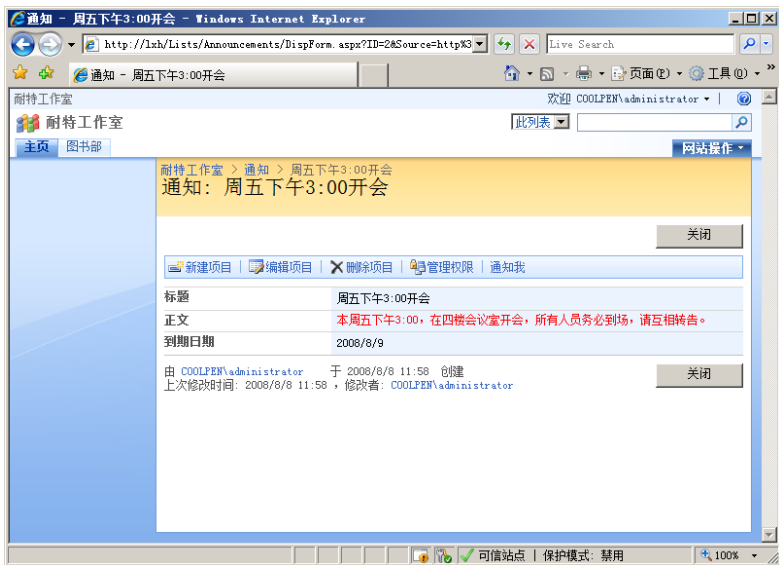


图 11-59 通知的属性

- ② 单击“编辑项目”按钮，打开通知编辑窗口。即可修改通知的内容，如图 11-60 所示。编辑完成后，单击“确定”按钮即可。

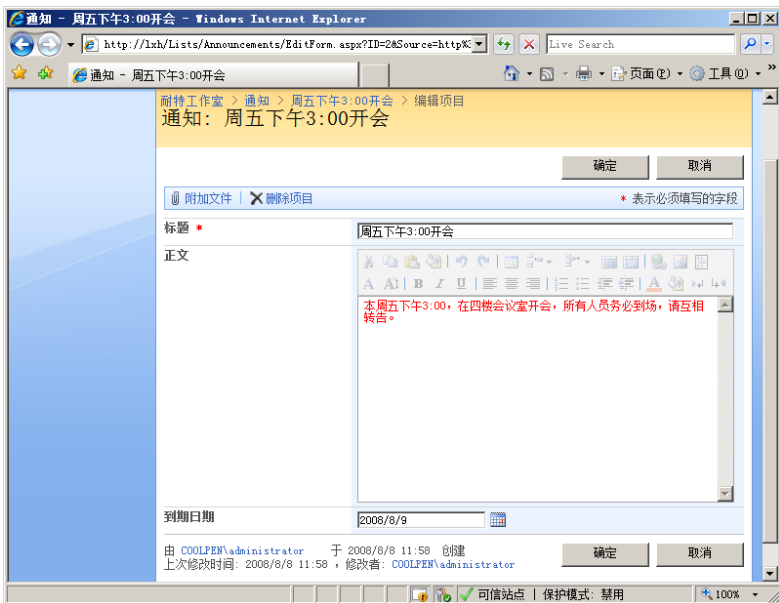


图 11-60 编辑通知

11.5.3 删除通知

如果通知设置了自动过期功能，那么到了规定日期后通知就会自动删除，不需要人为干预。不过，如果通知没有设置自动过期功能，则需要网络管理员手动删除。

在“通知”窗口中单击待删除的通知，打开通知属性窗口。单击“删除项目”按钮，显示如图 11-61 所示的提示框。单击“确定”按钮，即可将该通知删除。

需要注意的是，删除的通知并没有彻底从 WSS 网站中删除，而是放到了回收站中。在“网站设置”窗口中单击“网络集管理”选项组



图 11-61 提示框

域中的“回收站”超级链接，打开“网络集回收站”窗口。可看到所删除的通知，如图 11-62 所示。此时可以删除或者还原通知，也可以清空回收站。



图 11-62 “网络集回收站”窗口

11.6 事件管理

企业中经常会有一些事件发生或者通知，例如，每月的工资发放日、每周的例会日、各种法定或传统节日等，这些事件都可以在 WSS 网站中通过添加事件发布。而且由于这些事件每次发生的内容都几乎相同，所以不必每次都要重复添加。可以在 WSS 网站中一次创建这些事件，并且按照指定的时间发布。

11.6.1 添加事件

添加事件的操作步骤如下。

(1) 在 WSS 主页中单击“日历”选项组中的“添加新事件”超级链接，显示如图 11-63 所示的“日历：新建项目”窗口。在“重复”选项组中选中“将此事件设置为重复事件”复选框，然后选择事件发布的步骤及时间日期，设置为重复事件。在“标题”和“地点”文本框中分别输入事件的标题和地址，在“开始时间”和“结束时间”中设置事件的开始和结束时间，在“说明”文本框中输入事件内容。

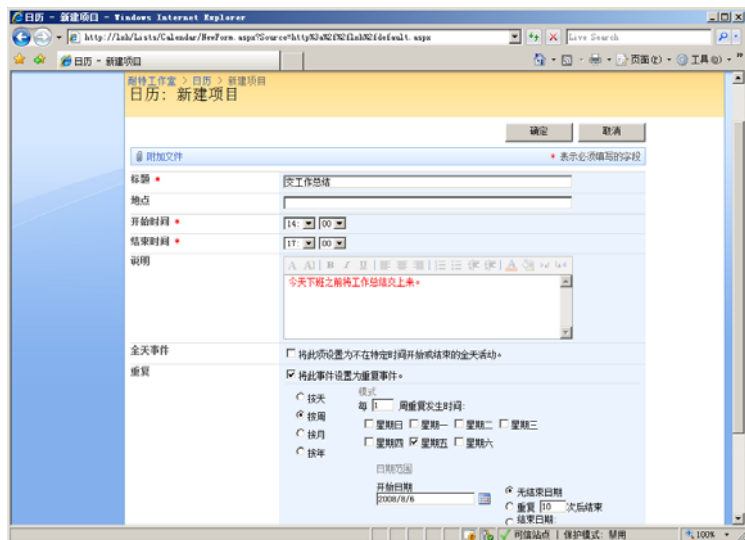


图 11-63 “日历：新建项目”窗口

(2) 单击“确定”按钮,创建完成新事件。在 WSS 网站主页中显示一系列未来事件,如图 11-64 所示。而当每个事件过期以后,就会自动从“日历”选项组中消失。

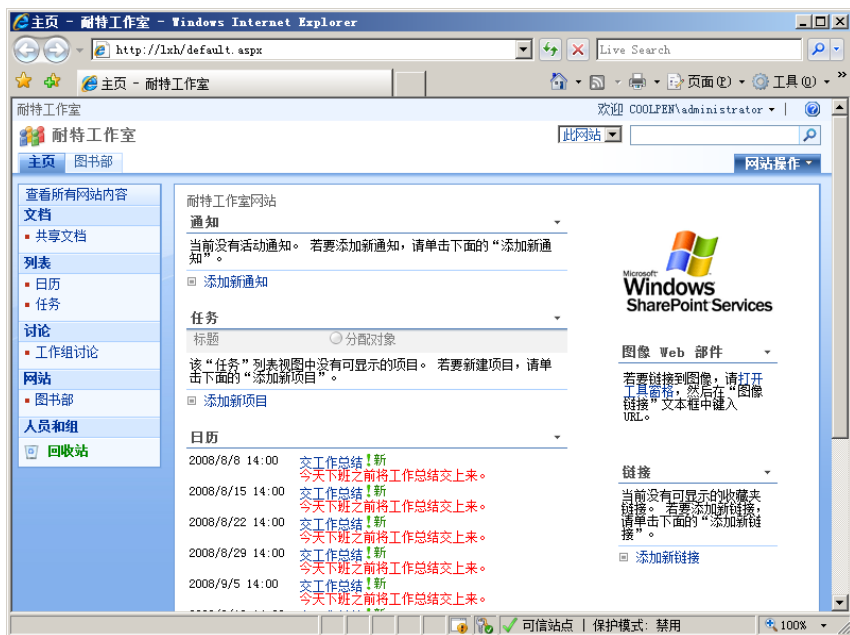


图 11-64 已发布的未来事件

11.6.2 修改与删除事件

已添加的事件也可以修改或者删除,不过重复事件和非重复事件的修改方式不同。修改普通事件时,只需单击“编辑项目”按钮;修改重复事件只需单击“编辑序列”按钮。

(1) 在 WSS 主页中单击待修改或删除的事件,显示如图 11-65 所示的事件属性窗口,其中列出所选事件的属性信息。



图 11-65 事件属性窗口

(2) 如果要删除该事件,单击“删除项目”按钮;如果要修改事件,则单击“编辑项目”按钮;

如果要修改的是重复事件，则单击“编辑序列”按钮，显示如图 11-66 所示的修改重复事件窗口，在其中所做的修改将应用于该重复事件。



图 11-66 修改重复事件窗口

11.7 管理与使用链接

网站中一般都会添加其他网页或网页的链接，如友情链接等。用户单击该链接时，即可直接打开相应的网站，从而起到方便访问及广告宣传等作用。在 WSS 网站中也可添加多个网站链接。

11.7.1 添加链接

添加链接的操作步骤如下。

① 在 WSS 主页中单击“链接”选项组中的“添加新链接”超级链接，显示如图 11-67 所示的“链接 - 新建项目”窗口。在“URL”文本框中添加要链接网站的 URL 地址，并输入说明信息。



图 11-67 “链接：新建项目”窗口

② 单击“确定”按钮，添加完成链接。按照同样的操作步骤，可以添加多个链接。所添加的链接将显示在 WSS 主页的“链接”选项组中，如图 11-68 所示。

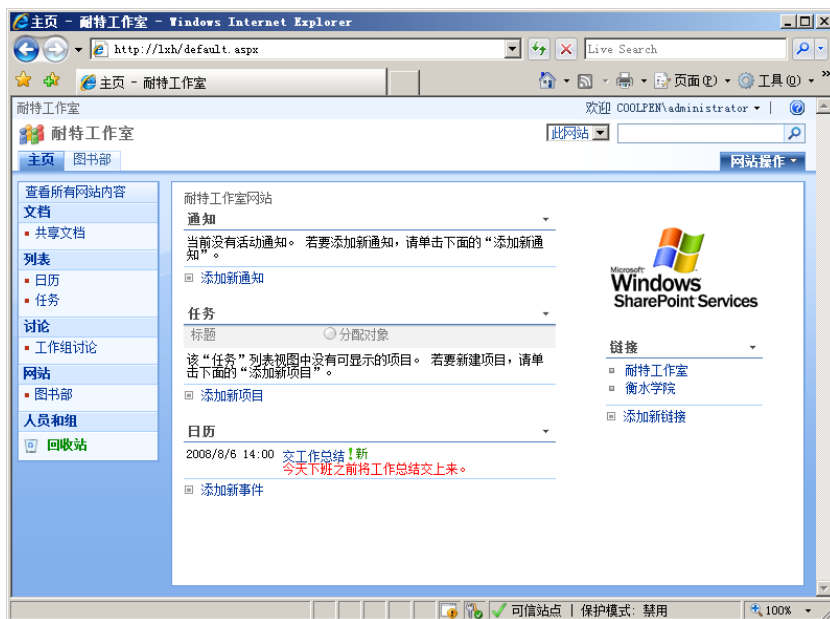


图 11-68 添加的链接

11.7.2 编辑链接

如果发现已添加的网站链接有错误，或者网址有所变动等，可以更改网络链接。在 WSS 主页中单击“链接”按钮，显示如图 11-69 所示的“链接”窗口，其中显示所有的链接。

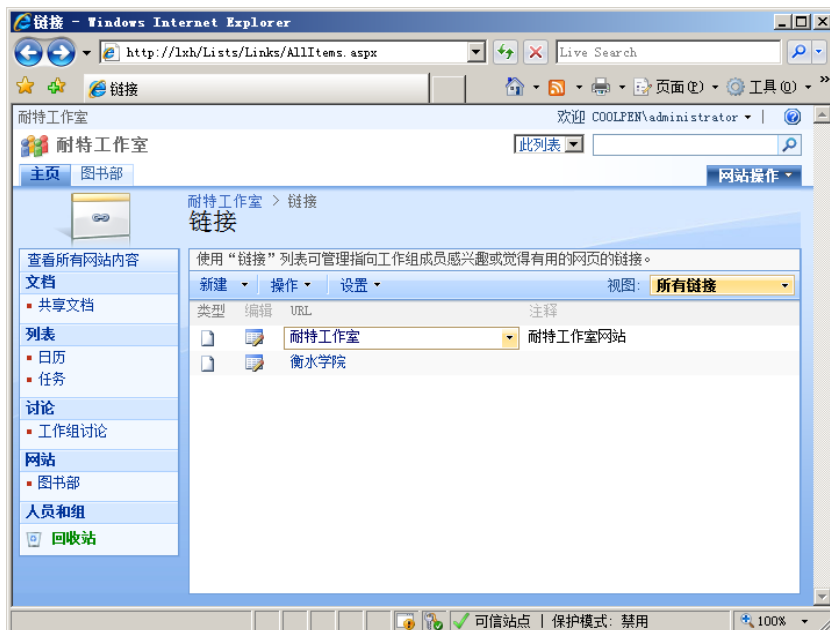


图 11-69 “链接”窗口

将鼠标指针移动到待更改的网站链接上，单击链接名称右侧的黑色箭头。在打开的下拉列表框中单击“编辑项目”选项，显示如图 11-70 所示的更改链接窗口，在其中可更改该链接的内容。

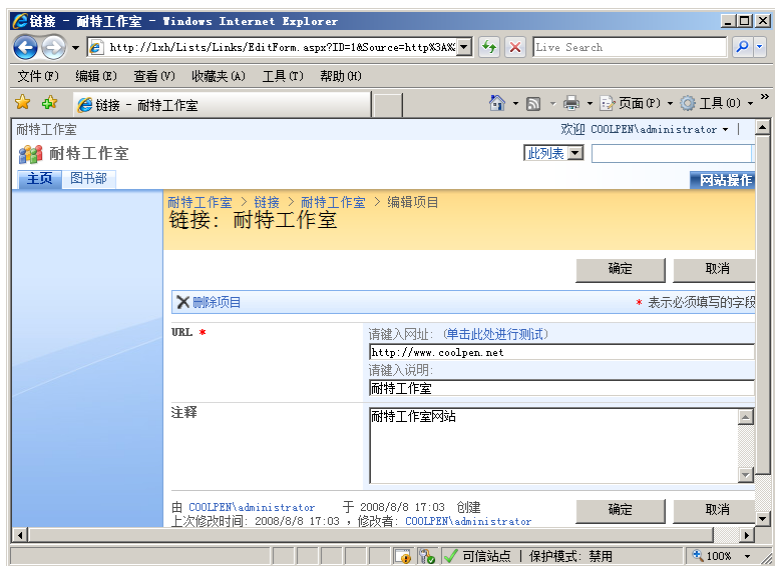


图 11-70 更改链接窗口

11.7.3 删除链接

如果要删除某个链接，则打开链接的下拉列表框，单击“删除项目”选项，显示如图 11-71 所示的提示框。单击“确定”按钮，即可将链接删除到回收站中。



图 11-71 提示框

11.7.4 修改链接 Web 部件

在 WSS 主页中，单击“链接”按钮右侧的黑色三角按钮。在下拉菜单中单击“修改共享 Web 部件”选项，显示如图 11-72 所示的共享 Web 部件窗口，在其中可根据需要设置链接部件的列表视图、外观、布局及高级等选项。

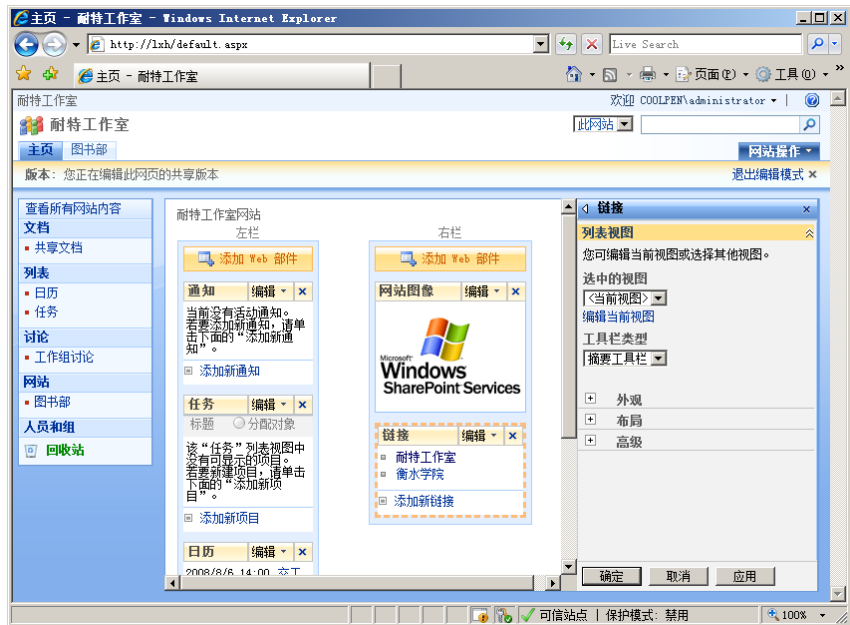


图 11-72 共享 Web 部件窗口

当设置完成以后，单击窗口右上方的“退出编辑模式”链接，应用所做的修改并退出编辑模式。

11.8 使用文档库

“库”是与网站用户共享文件的集合和保存体，通常应根据要共享的文件类型选择所需要的库。如果要共享数字图片或图形集合，则使用图片库；如果要存储一组基于 XML 的业务表格，则使用表单库；对于大多数的其他文件类型，如文档和电子表格，则使用文档库，该库是用户与工作组成员所共享的文件集合。

11.8.1 创建文档库

WSS 站点默认创建一个名为“共享文档”的文档库，用来共享文档，用户也可以根据自己的需要创建其他文档库。

(1) 在 WSS 主页中单击左侧栏中的“文档”按钮，显示如图 11-73 所示的“文档库”窗口，默认有一个“共享文档”。

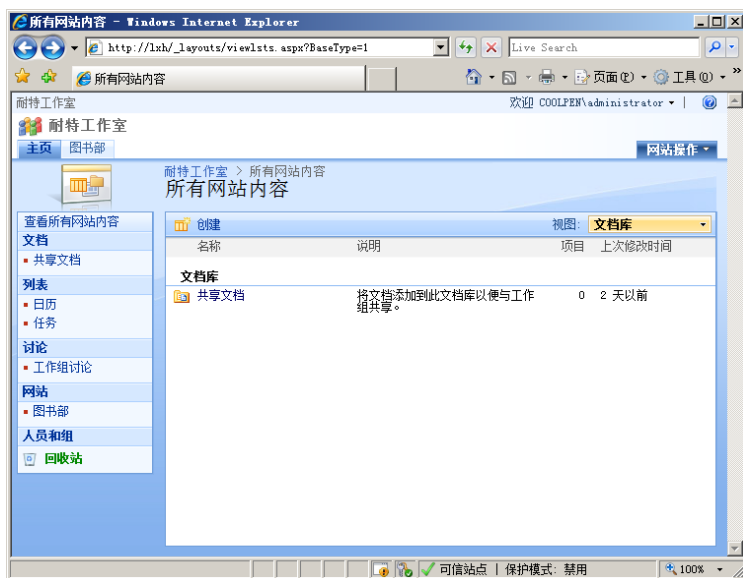


图 11-73 “文档库”窗口

(2) 单击“创建”按钮，显示如图 11-74 所示的“创建”窗口，在其中选择要创建的项目。



图 11-74 “创建”窗口

(3) 在“库”选项组中单击“文档库”超级链接，显示如图 11-75 所示的“新建”窗口，在“名称”和“说明”文本框中分别键入新文档库的名称和说明。

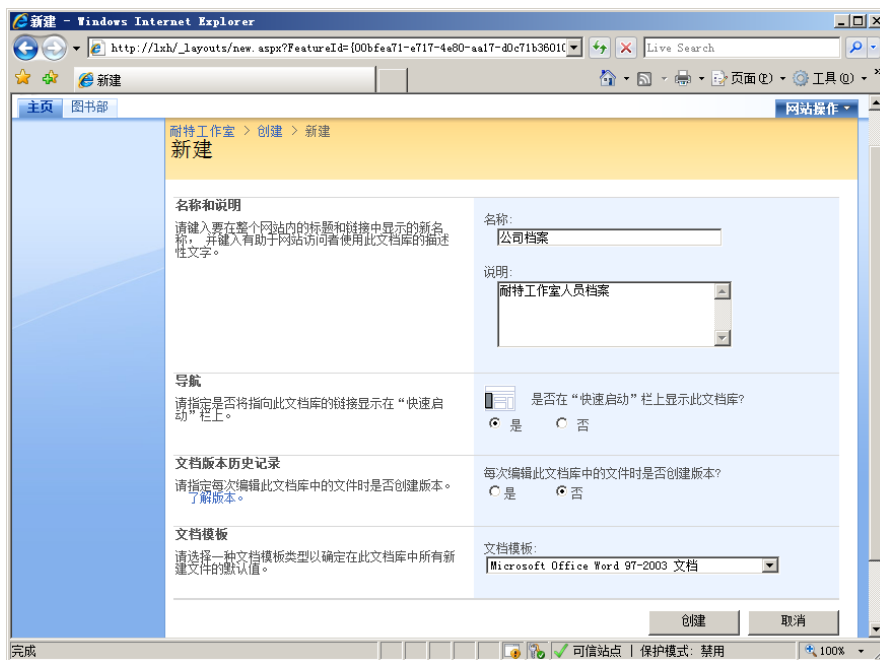


图 11-75 “新建”窗口

(4) 单击“创建”按钮，创建完成文档库，如图 11-76 所示，此时即可向该文档库中上传文档。



图 11-76 新文档库

11.8.2 修改和使用文档库

创建完成文档库以后，只是一个空文档库，用户可以为其上传文档或者直接在 Word 中将编辑的文档上传到文档库。如果对于已创建的文档库不满意，也可以修改文档库的内容。

1. 修改文档库

① 打开“文档库”窗口，单击“设置”按钮。在下拉菜单中单击“文档库设置”选项，显示如图 11-77 所示的“自定义”窗口。在其中可以修改文档库的常规设置、权限及视图等，也可以删除文档库。



图 11-77 “自定义”窗口

② 以更改标题说明为例。单击“常规设置”选项组中的“标题、说明和导航”超级链接，显示如图 11-78 所示的“文档库常规设置”窗口，在其中可更改该文档库的名称、说明及导航等。

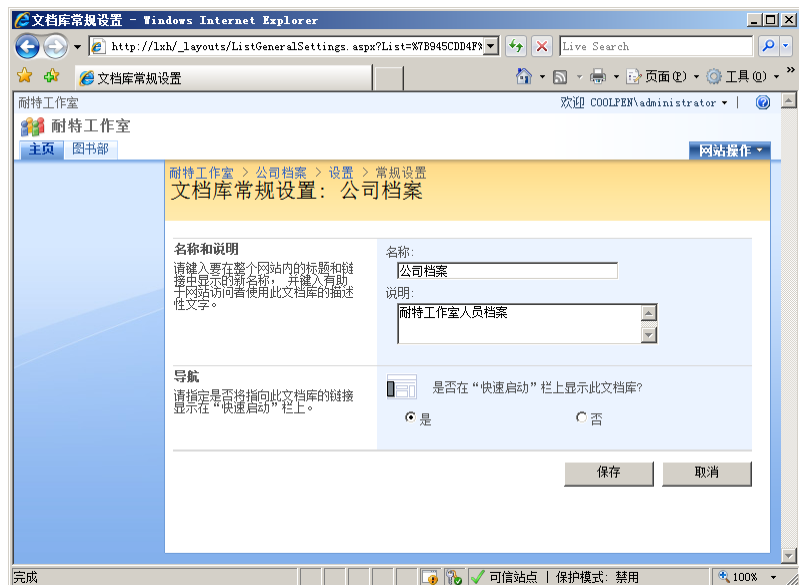


图 11-78 “文档库常规设置”窗口

③ 修改完成后单击“保存”按钮。

2. 上传文档

(1) 在新建的文档库窗口中单击“上传”按钮，显示如图 11-79 所示的“上传文档”窗口。单击“浏览”按钮，选择要上传的文档。

(2) 单击“确定”按钮，将该文档上传到文档库，如图 11-80 所示。按照同样的操作步骤，可继续上传其他文档。

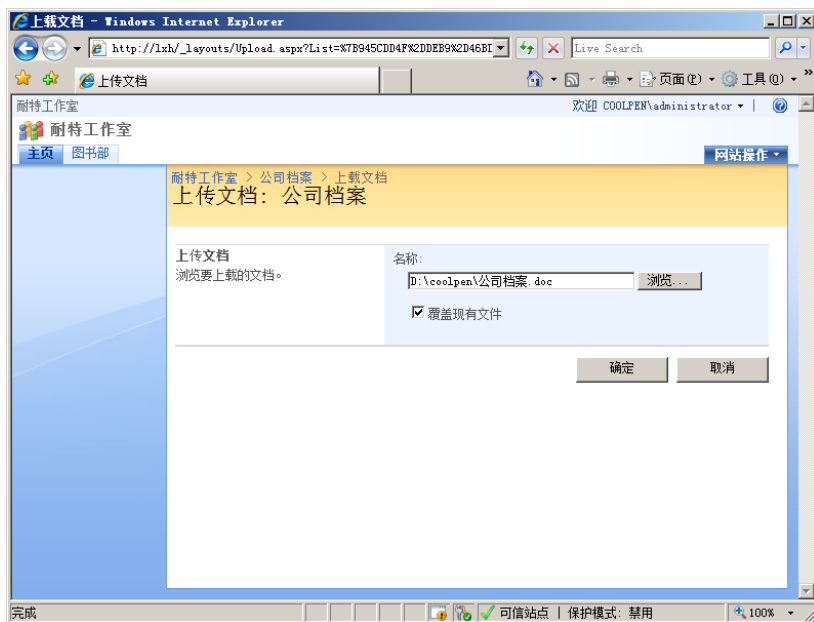


图 11-79 上传文档

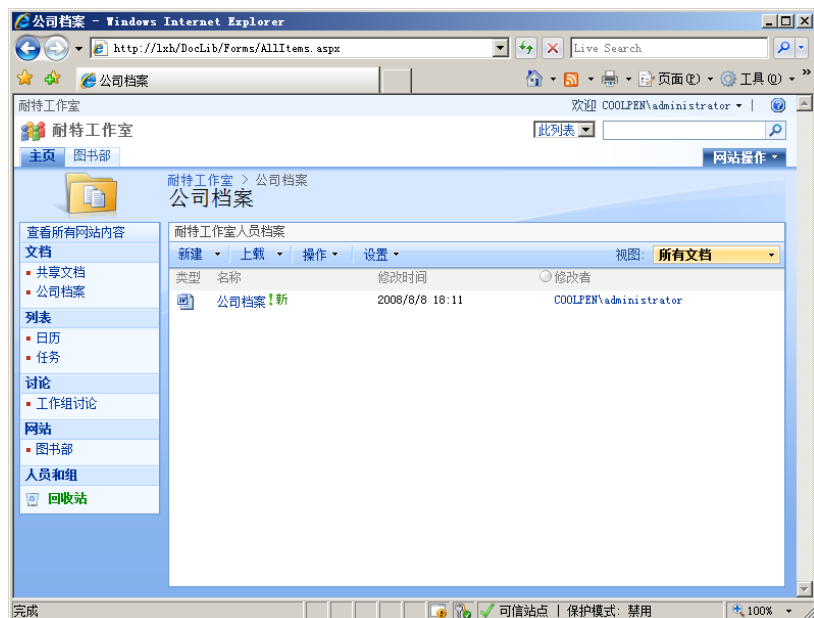


图 11-80 上传的文档

11.8.3 直接从 Word 中发布文档库

Word 内置了文档发布功能，可以将编辑的文档直接上传到 WSS 网站并创建一个文档工作区，而不必登录到 WSS 网站上传。不过为安全起见，在发布文档时必须首先将 WSS 网址地址添加到 IE 浏览器的信任区域。

① 打开 IE 浏览器，单击“工具”→“Internet 选项”选项，打开“Internet 选项”对话框。打开“安全”选项卡，如图 11-81 所示。

② 在“选择要查看的区域或更改安全设置”下拉列表框中选择“本地 Internet”选项，单击“站点”按钮，显示如图 11-82 所示的“本地 Internet”对话框。



图 11-81 “安全”选项卡

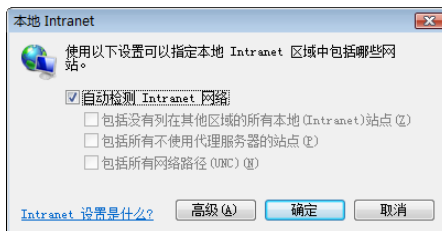


图 11-82 “本地 Intranet”对话框

③ 单击“高级”按钮，显示“本地 Intranet”对话框。在“将该网站添加到区域”文本框中输入 WSS 网站的网址，单击“添加”按钮添加到“网站”列表中，如图 11-83 所示。

④ 依次单击“关闭”和“确定”按钮，设置完成 IE 浏览器。

⑤ 在 Word 中编辑文档后单击“工具”→“共享工作区”选项，在窗口右侧显示“共享工作区”。在“文档工作区名称”文本框中键入 WSS 网站文档工作区的名称，在“新工作区位置”文本框中键入访问地址，如图 11-84 所示。

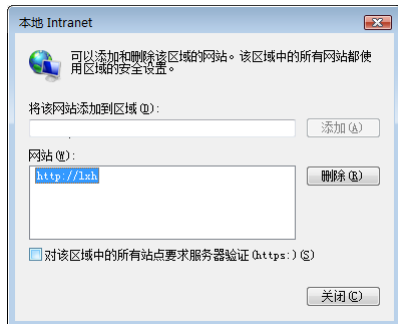


图 11-83 添加信任网站

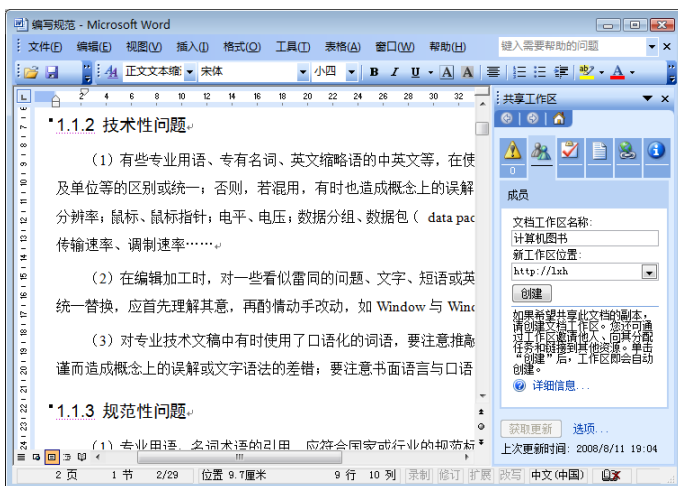


图 11-84 键入有关内容

⑥ 单击“创建”按钮，显示如图 11-85 所示的提示框，开始新建文档工作区。如果当前计算机没有加入域，则会显示要求键入用户名和密码的登录框；如果已经加入域并且以域用户登录，那么创建文档工作区就可以成功完成。

提示 如果没有将 WSS 网站添加为可信网站，那么在单击“创建”按钮创建文档工作区时显示如图 11-86 所示的警告框。

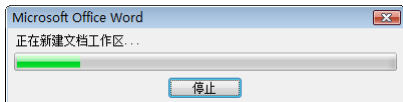


图 11-85 提示框



图 11-86 警告框

Word 文档发布成功，如图 11-87 所示，在“共享工作区”栏中显示该文档工作区的网址。

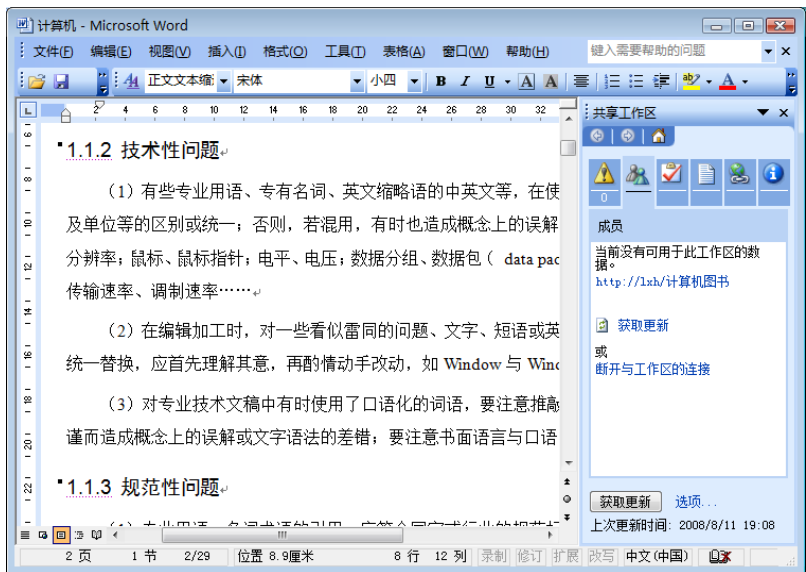


图 11-87 文档发布成功

⑦ 单击该网址，或者在 IE 浏览器中直接输入该网站即可登录到该文档工作区，如图 11-88 所示。单击文档名称，即可在 Word 中打开并编辑，也可以在该工作区中添加新文档。

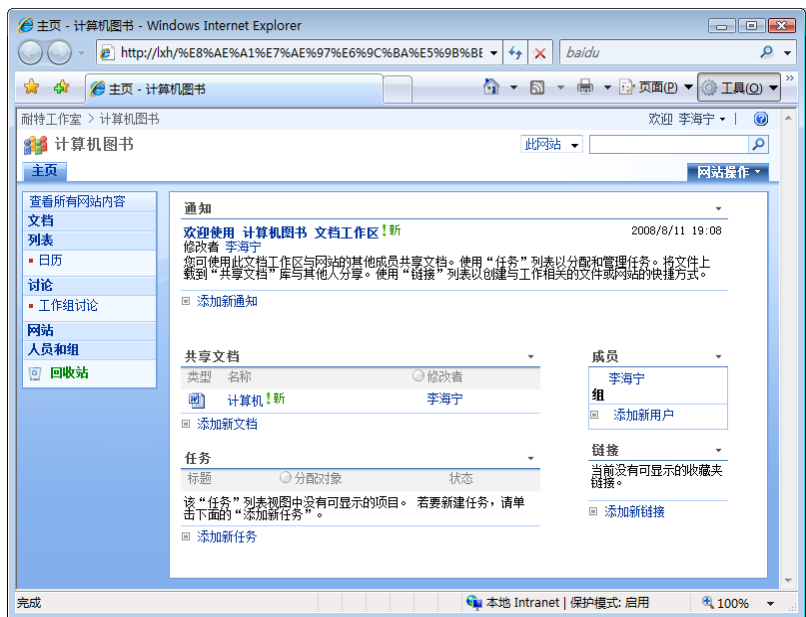


图 11-88 文档工作区

如果修改了服务器中的文档，那么需要在本地计算机上获取更新，以保持文档的同步。在 Word 中打开该文档以后，单击“获取更新”按钮，即可将该文档与服务同步。

11.9 使用列表

在 WSS 网站中，列表是用户与工作组成员共享的信息集合。SharePoint 工作组网站默认包括了一组内置列表库，如链接、任务、日历和通知等。默认情况下，列表中没有包含任何内容。用户可以创建列表，或者在列表中添加内容等。例如，可以为事件创建签约表，或者创建建议列表等。

11.9.1 创建列表

创建列表的操作步骤如下。

① 在 WSS 主页中单击左侧栏中的“列表”按钮，显示如图 11-89 所示的“列表”窗口，其中列出已包含的列表。



图 11-89 “列表”窗口

② 单击“创建”按钮，显示如图 11-90 所示的“创建”窗口，在其中选择在现有列表中添加的新列表库。



图 11-90 “创建”窗口

③ 单击“自定义列表”选项组中的“自定义列表”超级链接，显示如图 11-91 所示的“新建”窗口，在“名称”和“说明”文本框中分别输入列表名称和说明即可。

④ 单击“创建”按钮，图片库创建完成，如图 11-92 所示，此时即可在其库中添加内容。

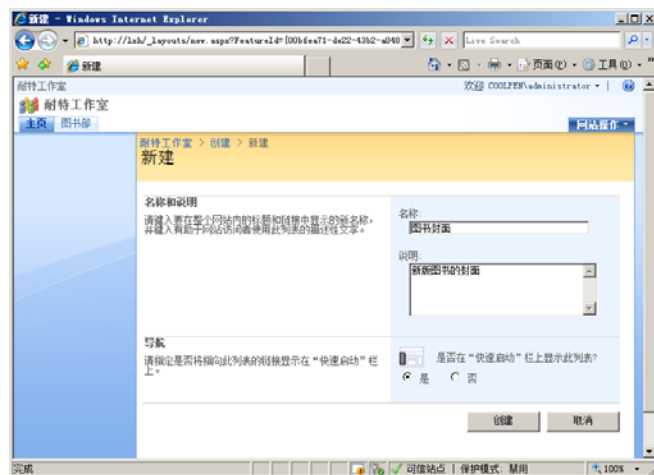


图 11-91 “新建”窗口

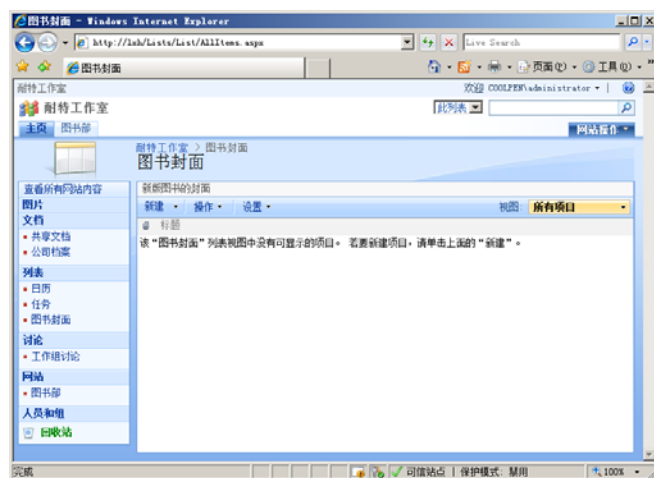


图 11-92 新创建的图片库

11.9.2 修改列表

打开要修改的列表窗口，单击“设置”按钮。在下拉菜单中选择“列表设置”选项，显示如图 11-93 所示的“自定义”窗口。在其中可以修改该列表库的常规设置及权限等，与设置文档库类似。

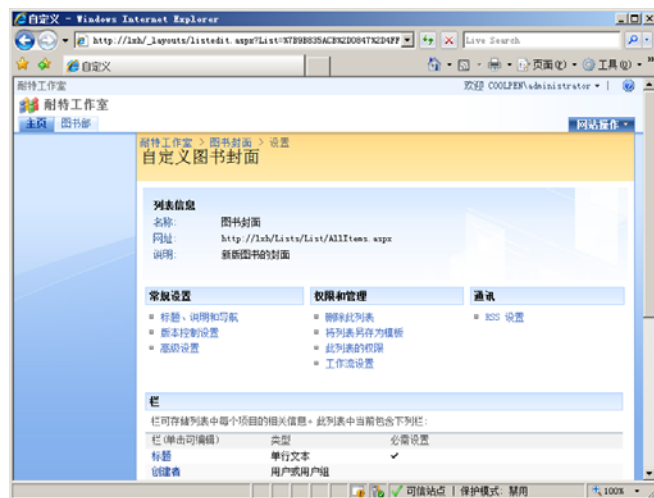


图 11-93 “自定义”窗口

11.9.3 在 Excel 中直接发布列表

在 Word 中可以向 WSS 网站发布 Word 文档，同样在 Excel 中同样也可以发布列表。

① 在 Excel 中打开文档，选中表格。右击并选择快捷菜单中的“创建列表”选项，显示如图 11-94 所示的“创建列表”对话框。

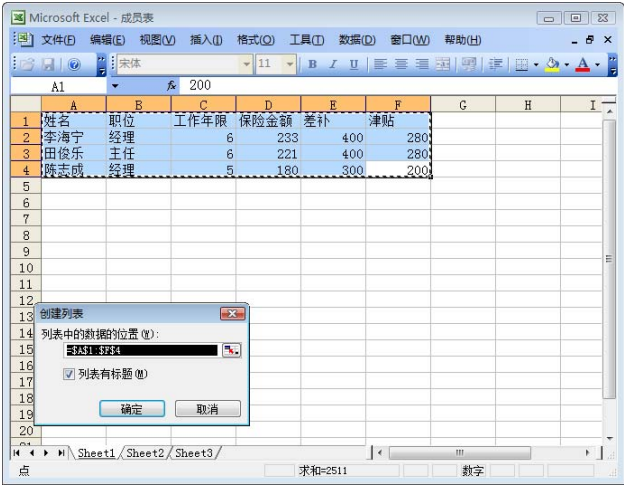


图 11-94 “创建列表”对话框

② 单击“确定”按钮，关闭该对话框。再次右击选中的表格，在快捷菜单中选择“列表”→“发布列表”选项，显示如图 11-95 所示的“发布列表到 SharePoint 网站”对话框。在“地址”文本框中键入 WSS 网站地址，在“名称”文本框中输入文档标题。

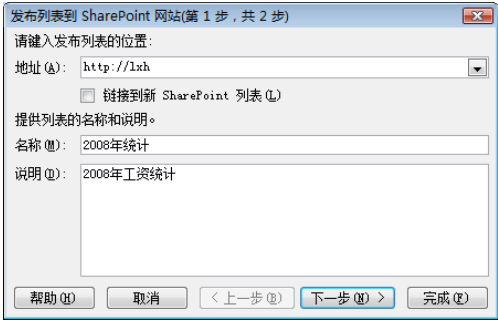


图 11-95 “发布列表到 SharePoint 网站”对话框

③ 单击“下一步”按钮，显示如图 11-96 所示的对话框，提示需要验证所列出的列是否与正确的数据类型关联。

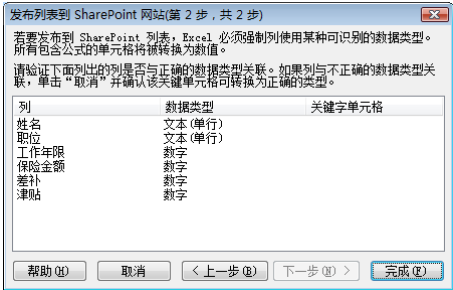


图 11-96 提示需要验证列表中的列

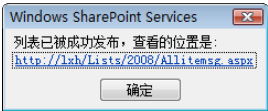


图 11-97 提示框

④ 单击“完成”按钮，显示如图 11-97 所示的提示框。提示列表已被成功发布，并显示列表的发布地址。

⑤ 单击超级链接，或者在 IE 浏览器中直接输入该超级链接地址，即可打开包含该列表的网页，如图 11-98 所示。此时，即可在线实时修改列表网站中的数据。

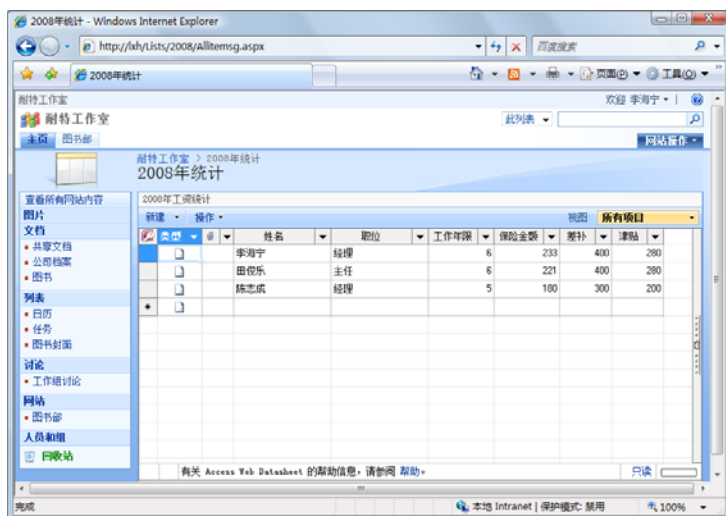


图 11-98 包含列表的网页

11.10 使用 Microsoft 提供的 WSS 模板

虽然 WSS 内置了多个模板，但并不一定能够满足用户的需要。因此微软公司为 WSS 服务提供了许多模板。尤其是为中国用户定制了 12 款 WSS 中文模板，并且可以免费下载。这样一来，用户就可以根据自己的需要直接从微软网站上下载需要的模板。然后上传到自己的 WSS 网站，用来创建自己的站点。

11.10.1 WSS 模板功能

微软此次发布的 WSS 中文模板主要包括政府部门、企业销售部门、企业人事部门、企业 IT 技术部门及学校班级网站模板等，专为中国的大中小企业、政府部门、学校等各类用户以及销售、人力资源或财务等特定工作团队量身打造。

微软提供的中文 WSS 模板下载页面如图 11-99 所示，下载地址为：

<http://office.microsoft.com/zh-cn/assistance/HA011929182052.aspx>



图 11-99 WSS 模板下载页面

用户可以预览这些模板，并可以将其下载到本地计算机上。下载以后，需要解压缩才能使用。操作步骤如下。

- ① 运行所下载的模板程序，显示如图 11-100 所示的许可协议对话框，提示阅读许可协议。
- ② 单击“是”按钮，显示如图 11-101 所示的对话框。单击“浏览”按钮，选择模板文件的保存路径。

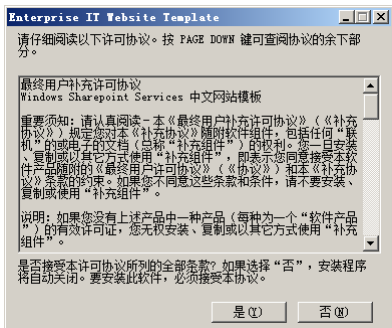


图 11-100 许可协议对话框

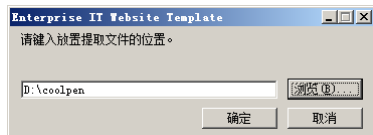


图 11-101 保存路径

- ③ 单击“确定”按钮，解压缩完成。

11.10.2 上传模板到 WSS 网站

上传模板到 WSS 网站的操作步骤如下。

- ① 打开“网站设置”窗口，在“库”选项组中单击“网站模板”超级链接，显示如图 11-102 所示的“网站模板库”窗口。



图 11-102 “网站模板库”窗口

- ② 单击“上传”按钮，显示如图 11-103 所示的“上传模板”窗口，单击“浏览”按钮选择要上传的模板。
- ③ 单击“确定”按钮，即可将模板上传到 WSS 网站。完成后显示如图 11-104 所示的窗口，在其中可以设置新模板的名称、标题和说明信息。
- ④ 设置完成后单击“确定”按钮，一个模板上传成功，如图 11-105 所示。重复上述操作，可继续上传其他模板。

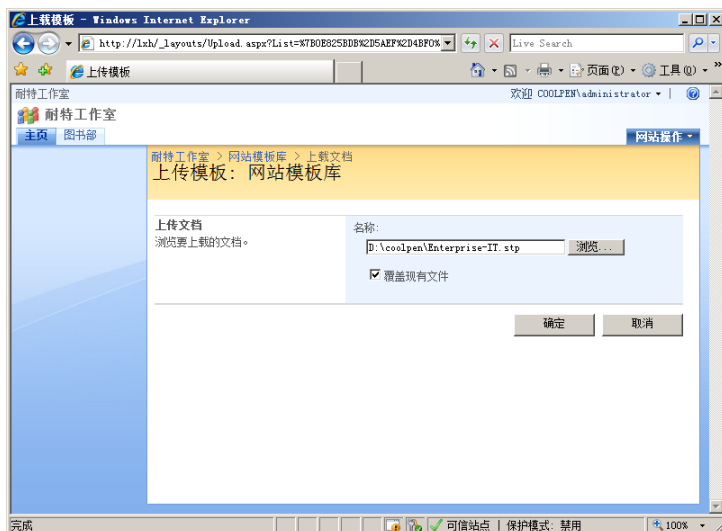


图 11-103 “上传模板”窗口

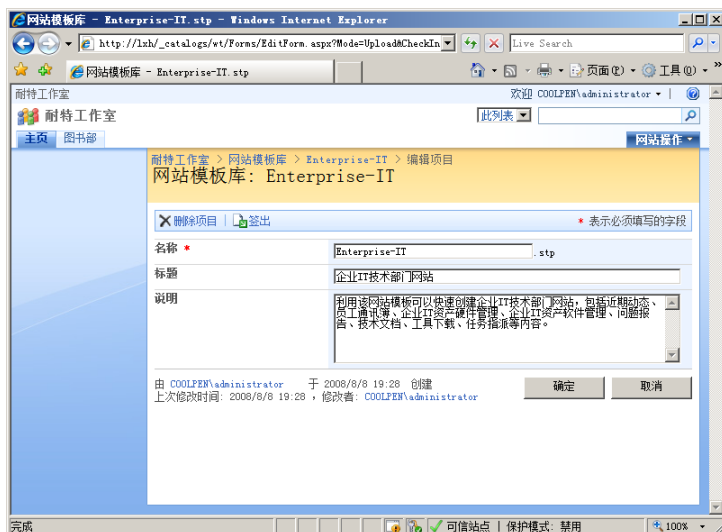


图 11-104 设置模板属性

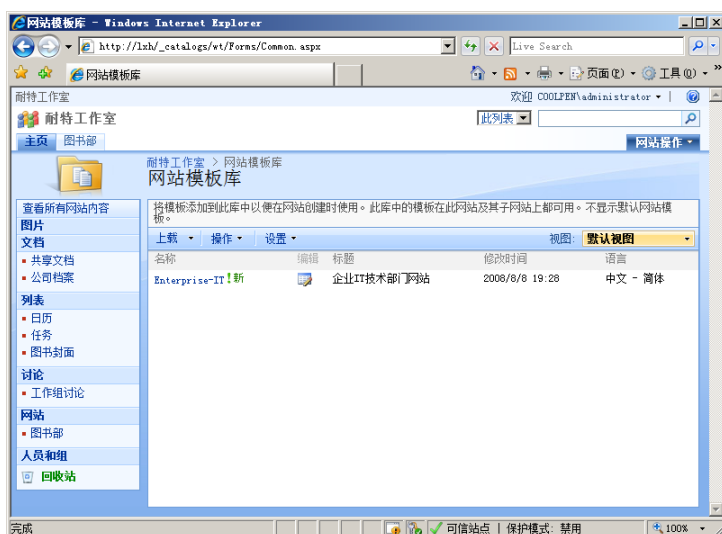


图 11-105 已上传的模板

11.10.3 使用 WSS 模板创建站点

WSS 模板创建完成以后，在创建新站点的时候可选择上传的新模板，具体操作请参见前面所述内容。

11.11 Windows Server 2003 R2/2008 的配置差异

在 Windows Server 2003 R2 系统中 WSS 作为内置服务已被集成在其中，并且版本为 WSS 2.0，无顺下载即可安装使用。没有安装 R2 的 Windows Server 2003 系统，则没有集成 WSS 功能。

运行“配置您的服务器向导”，在“服务器角色”对话框中选择“SharePoint Services”选项，如图 11-106 所示，即可成功安装 WSS。

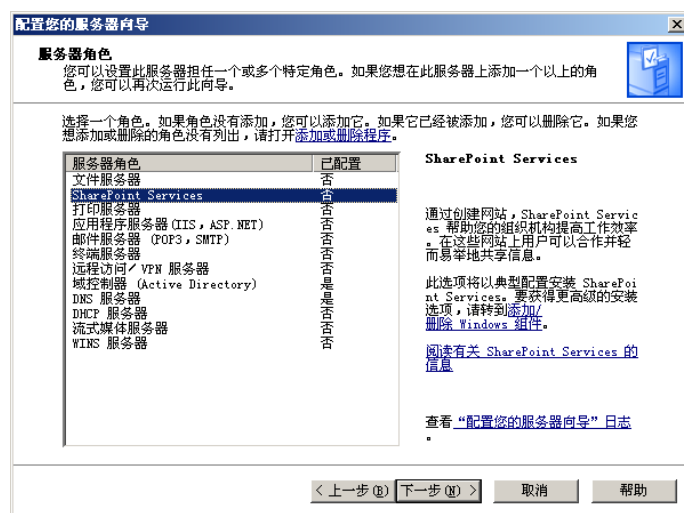


图 11-106 选择“SharePoint Services”选项

WSS 安装完成后，即可登录到 WSS 站点并配置。Windows Server 2003 R2 中的 WSS 与 Windows Server 2008 中的 WSS 无论是界面，还是功能都非常类似，如图 11-107 所示。



图 11-107 Windows Server 2003 R2 中的 WSS

具体操作步骤可参见前面所述内容。

第 12 章 配置与管理证书和认证服务

随着网络的发展，安全隐患也越来越多。尤其是在一些允许未经授权用户访问的网络，一旦数据被人截获、篡改或假冒等，对企业 and 用户都带来难以预料的恶劣后果。因此安全问题也越来越被人们所重视，特别是电子交易网站。电子证书是一种应用非常广泛的提高通信安全性的方式，可以实现用户身份认证及数据加密等功能，从而保护用户的网络及传输信息的安全。

12.1 电子证书和认证服务概述

要利用电子证书实现网络安全通信，必须要搭建认证服务器，安全 Web 连接的站点（使用 HTTPS）、邮件的签名和加密，以及网上银行在线交易等都需要证书来保护用户或计算机的安全。Windows Server 2008 自带了证书服务功能，可以颁发不同类型数字证书，用户使用颁发的证书即可实现安全连接及数据加密等功能。

12.1.1 数字证书简介

证书类似于生活中的“证书”，都是由信任的证书颁发机构或第三方机构颁发的，并且不同的证书只能应用于其特定的领域。数字证书则是一段由证书颁发机构（Certification Authority, CA）数字签名并且包含用户身份信息 and 用户公钥信息，以及身份验证机构数字签名的数据，用来代表用户的身份。其中身份验证机构的数字签名可以确保证书信息的真实性，而用户公钥信息可以保证数字信息传输的完整性，用户的数字签名可以保证数字信息的不可否认性。

证书的主要功能是向网络上的其他用户证明个人身份，用于网络上身份验证及保证公开网络上信息安全。每个证书都拥有可以公开的“公钥”及与之相关联的私钥，同时只有证书持有人才拥有“私钥”。证书将公钥安全地绑定到持有相应私钥的实体中，并通过网络传输。证书由证书颁发机构（CA）管理，此过程称为“签名”，而且证书可以颁发给用户、计算机或某一应用程序。

Windows Server 2008 使用公共密钥基础结构（Public Key Infrastructure, PKI）来处理企业内部或外部网络中用户的身份验证、数据加密及数字签名等。公共密钥属于“非对称加密”技术，使用“公钥”和“私钥”两个密钥。其中“公钥”可以对所有用户公开；而“私钥”则必须由使用者自己秘密保存，不能泄露。这两个密钥彼此相关联，通常都是通过证书来发布的。

用户在发送信息时，可以使用自己的“私钥”为发送的电子邮件及文档等进行“签名”。如果数据在传送的过程中被更改，则收到的电子邮件及文档中的“签名”信息将不复存在。而接收者也将看不到发送者的“签名”信息，这样接收者就可以判断所接收到的信息是否被“篡改”。当然发送者也可以使用接收者的“公钥”加密发送的数据，只有接收者使用自己的“私钥”才能解密。这样即使其他人通过各种途径收到该数据，由于没有对应的私钥也不能查看数据内容，从而保证了数据的安全。

12.1.2 认证服务简介

Windows Server 2008 支持两种证书服务器，分别是应用于企业内部的企业证书服务器和用于企业或 Internet 的独立证书服务器。其中企业证书服务器应用于域环境，需要 Windows Server 2008 活动目录（Active Directory）的支持，用户可以直接向证书服务器申请并安装证书；独立根证书服务器应用于非域环境，可以安装在任何一台独立服务器上，但用户向证书服务器申请证书时必须由管理员检查后颁发才能使用。

需要注意的是，在部署了证书服务后服务器的计算机名和域名都不能更改，但可以更改 IP 地址。

12.2 电子证书服务

Windows Server 2008 支持两种证书服务，分别是用于企业内部的企业证书服务器（企业 CA）和用于企业或 Internet 网络中的独立的证书服务器（独立 CA）。企业 CA 需要 Windows Server 2008 活动目录的支持，而独立 CA 可以安装在任何独立的 Windows Server 2008 计算机中。

12.2.1 安装企业 CA

证书服务作为 Windows Server 2008 的内置组件，默认情况下并没有安装。由于企业证书服务器需要活动目录的支持，因此在安装企业证书服务器时必须首先安装域服务。

① 运行“添加角色向导”，当显示如图 12-1 所示的“选择服务器角色”对话框时在“角色”列表框中选中“Active Directory 证书服务”复选框。



图 12-1 “选择服务器角色”对话框

② 单击“下一步”按钮，显示如图 12-2 所示的“Active Directory 证书简介”对话框，其中显示证书服务的简介及注意事项。



图 12-2 “Active Directory 证书简介”对话框

③ 单击“下一步”按钮，显示如图 12-3 所示的“选择角色服务”对话框。在其中选择为 Active Directory 证书服务安装的角色服务，默认选中“证书颁发机构”复选框。

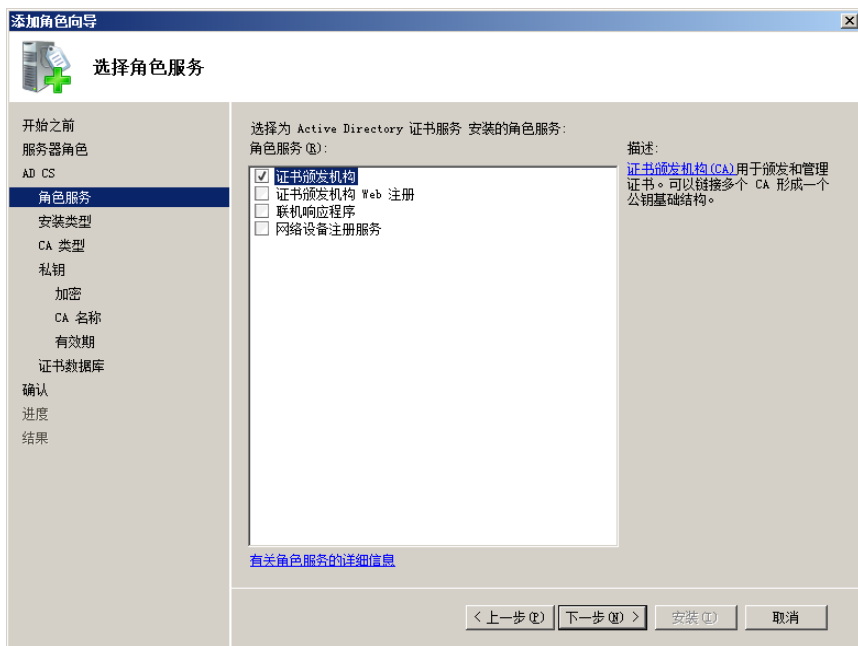


图 12-3 “添加角色服务”对话框

④ 如果要启用证书 Web 注册功能，则选中“证书颁发机构 Web 注册”复选框。由于证书 Web 注册需要启用 Web 功能，因此会显示如图 12-4 所示的对话框，需要添加 Web 服务器功能。



图 12-4 添加 Web 服务器功能



注意： 只有 Windows Server 2008 企业版和数据中心版支持 Web 注册功能，标准版和 Web 版则不支持。



⑤ 单击“添加必需的角色服务”按钮，显示如图 12-5 所示的“指定安装类型”对话框。选择“企业”单选按钮，用来安装企业证书。

⑥ 单击“下一步”按钮，显示如图 12-6 所示的“指定 CA 类型”对话框。由于是第 1 次安装，并且是唯一的证书颁发机构，因此选择“根 CA”单选按钮。

⑦ 单击“下一步”按钮，显示如图 12-7 所示的“设置私钥”对话框。由于现在是第 1 次安装证书服务，并且没有私钥，因此选择“新建私钥”单选按钮。

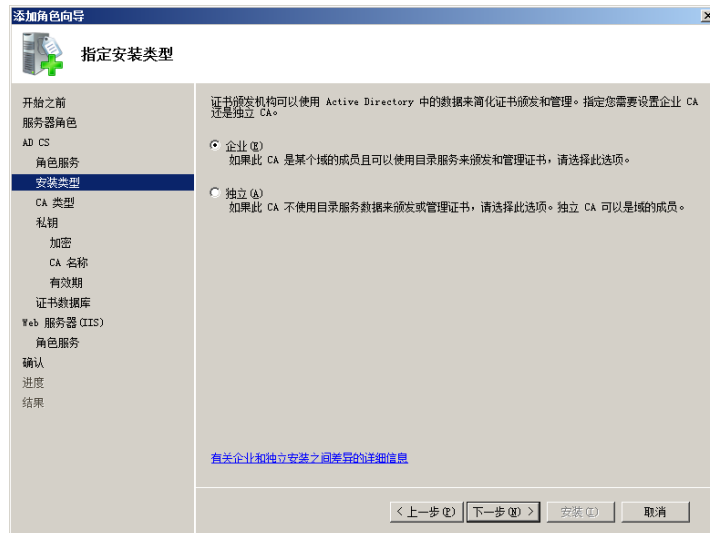


图 12-5 “指定安装类型”对话框

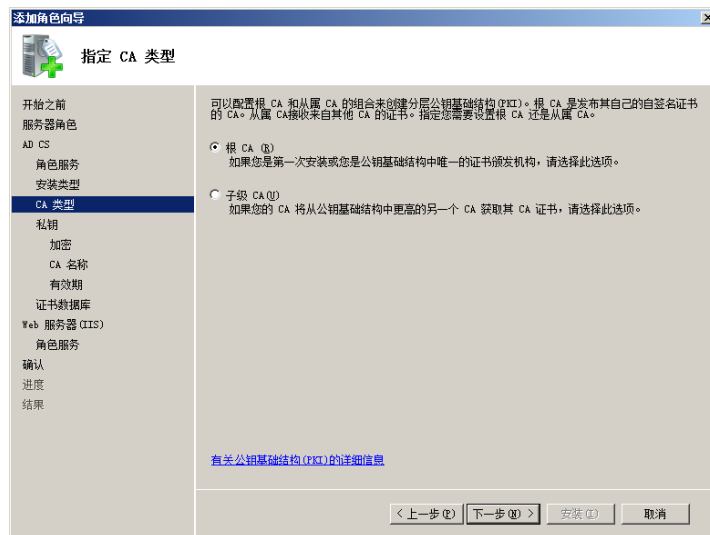


图 12-6 “指定 CA 类型”对话框



图 12-7 “设置私钥”对话框

⑧ 单击“下一步”按钮，显示如图 12-8 所示的“为 CA 配置加密”对话框。在“选择加密服务提供程序”下拉列表框中选择加密程序，在“密钥字符长度”下拉列表框中选择密钥长度，在“选择此 CA 颁发的签名证书的哈希算法”下拉列表框中选择要使用的哈希算法。

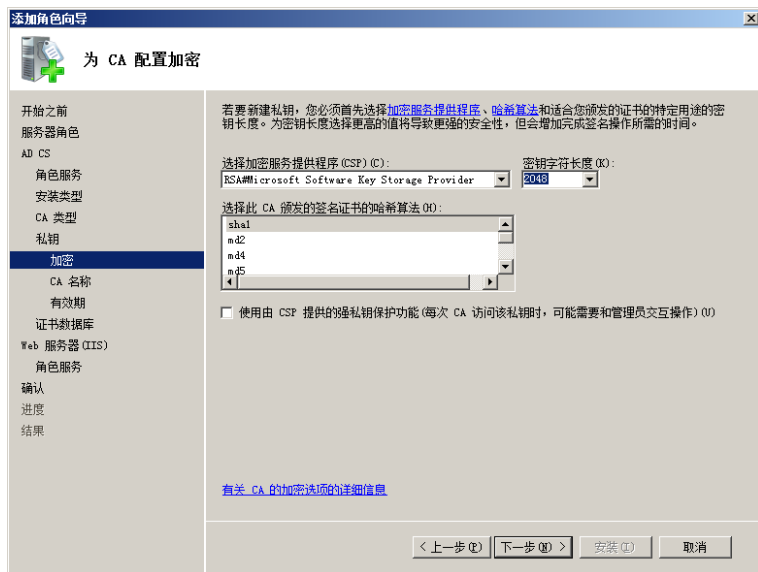


图 12-8 “为 CA 配置加密”对话框

⑨ 单击“下一步”按钮，显示如图 12-9 所示的“配置 CA 名称”对话框，在“此 CA 的公用名称”文本框中设置此证书的公用名称。



图 12-9 “配置 CA 名称”对话框

⑩ 单击“下一步”按钮，显示如图 12-10 所示的“设置有效期”对话框。设置该证书的有效期，默认为 5 年。

⑪ 单击“下一步”按钮，显示如图 12-11 所示的“配置证书数据库”对话框，在其中设置证书数据库和数据库日志的位置。

⑫ 由于要同时安装“证书颁发机构 Web 注册”功能，因此单击“下一步”按钮，显示如图 12-12 所示的“Web 服务器 (IIS)”对话框，其中显示 IIS 的简介信息。

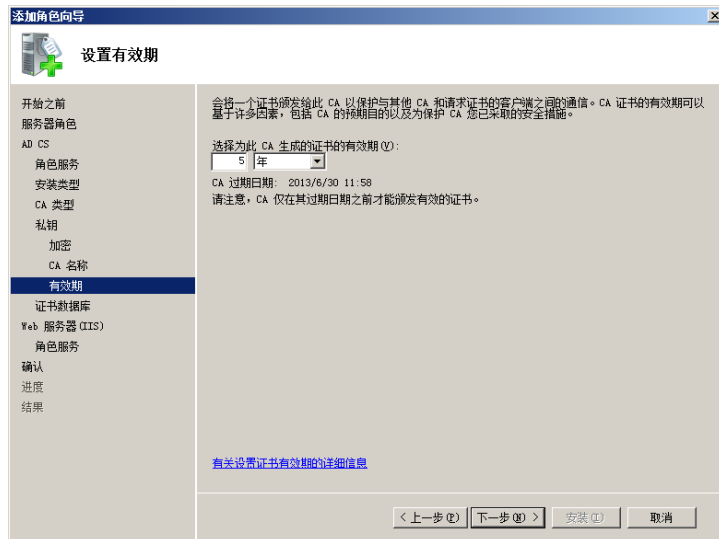


图 12-10 “设置有效期”对话框



图 12-11 “配置证书数据库”对话框



图 12-12 “Web 服务器 (IIS)”对话框

⑬ 单击“下一步”按钮，显示如图 12-13 所示的“选择角色服务”对话框。在其中选择要安装的 IIS 组件，保留默认设置即可。

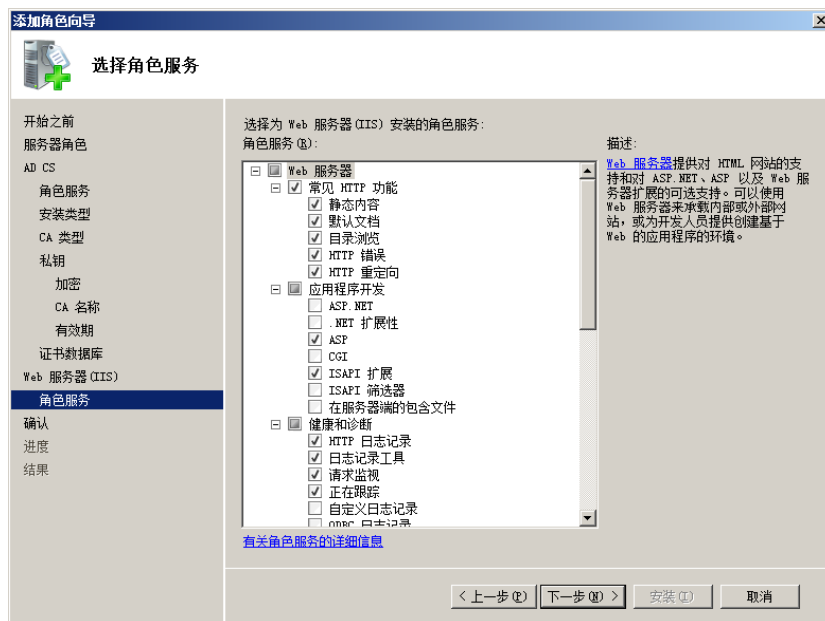


图 12-13 “选择角色服务”对话框

⑭ 单击“下一步”按钮，显示如图 12-14 所示的“确认安装选择”对话框。其中列出要安装的角色，同时提示用户安装证书服务以后，将无法更改计算机的名称和域设置。



图 12-14 “确认安装选择”对话框

⑮ 单击“安装”按钮，开始安装证书服务及相关组件。安装完成以后，显示如图 12-15 所示的“安装结果”对话框。

⑯ 单击“关闭”按钮，安装完成证书服务。

打开“服务器管理器”窗口，依次展开“角色”→“Active Directory 证书服务”选项。查看所安装的证书服务，如图 12-16 所示。



图 12-15 “安装结果”对话框

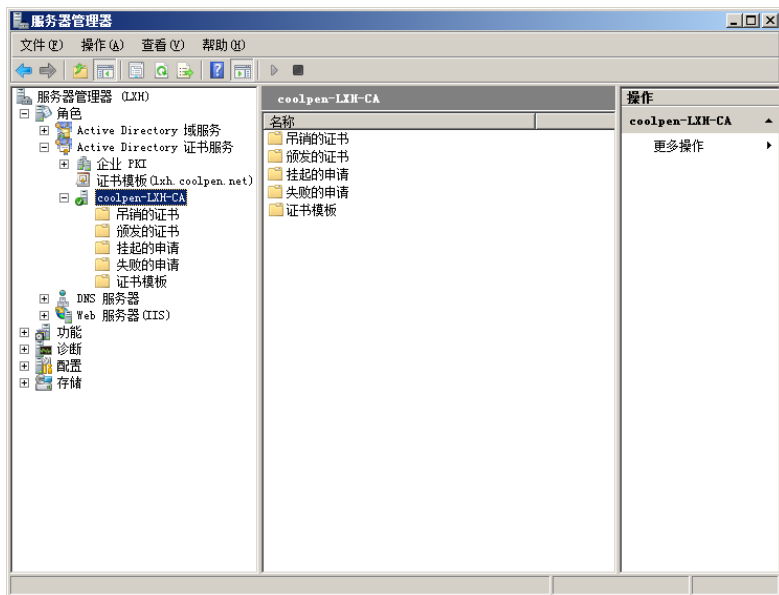


图 12-16 安装证书服务

12.2.2 安装独立根 CA

如果网络内尚未安装域服务，也可以将证书服务安装在独立服务器上，从而实现证书的颁发与管理。不过由于独立根 CA 不需要 Active Directory，因此只能使用 Web 方式注册证书。无法利用“证书申请向导”，而且所申请的证书必须经由管理员颁发。

(1) 以管理员用户身份登录到服务器，运行“添加角色向导”，在“选择服务器角色”对话框中选择“Active Directory 证书服务”复选框。

(2) 在如图 12-17 所示的“选择角色服务”对话框中选中“证书颁发机构”和“证书颁发机构 Web 注册”复选框启用 Web 注册功能。

(3) 在如图 12-18 所示的“指定安装类型”对话框中选择“独立”单选按钮。由于此服务器不是域控制器，并且未加入域，因此“企业”单选按钮为灰色不可选状态。

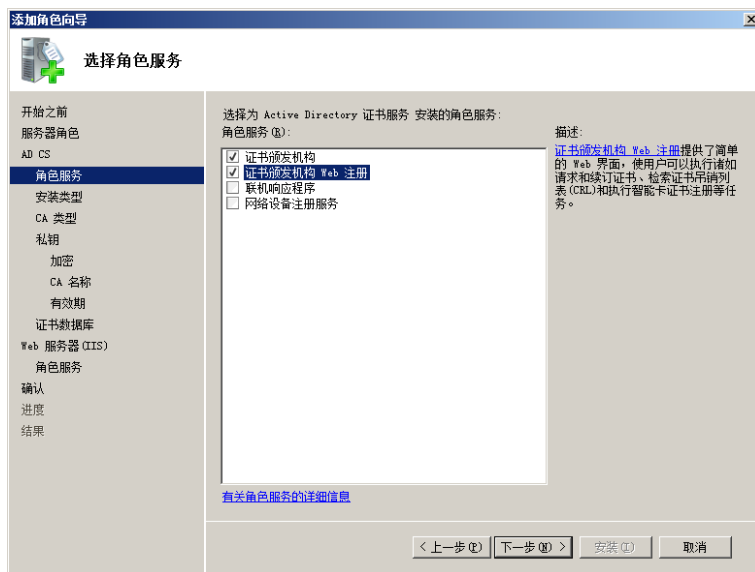


图 12-17 “选择角色服务”对话框

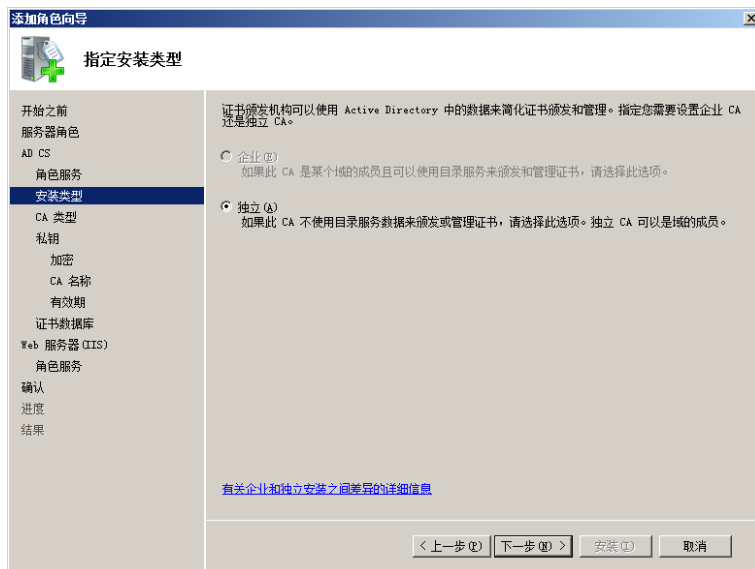


图 12-18 “指定安装类型”对话框

其他操作与安装企业 CA 完全相同，这里不再赘述。

12.3 使用企业证书服务

证书服务器安装完成以后，无论是域成员用户，还是非域成员用户都可以向证书服务器申请证书。申请证书可以使用 Web 方式或“证书申请向导”两种方式，前者无论是域成员用户还是非域成员用户都可使用；而后者只有加入域以后才能使用。

12.3.1 使用 Web 方式申请与安装证书

如果在安装证书服务器的同时，也安装了“证书颁发机构 Web 注册”，那么就可以通过 Web 方式来申请证书，而且不需要加入域，但需要配置信任证书服务器才能安装证书。域用户不必配置证书服务信任即可安装证书，申请证书的客户端可以使用 Windows 2000/XP/Vista 操作系统，这里以 Windows Vista 系统为例。

1. 配置 IE 浏览器

① 使用管理员用户登录 Windows Vista，首先需要使 IE 浏览器能够运行 ActiveX 控件。打开 IE 浏览器，单击“工具”→“Internet 选项”选项，显示“Internet 选项”对话框。打开“安全”选项卡，如图 12-19 所示。

② 单击“自定义级别”按钮，显示如图 12-20 所示的“安全设置 – Internet 区域”对话框，将“对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本（不安全）”和“允许运行以前未使用的 ActiveX 控件而不提示”均选择为“启用（不安全）”单选按钮。



图 12-19 “安全”选项卡

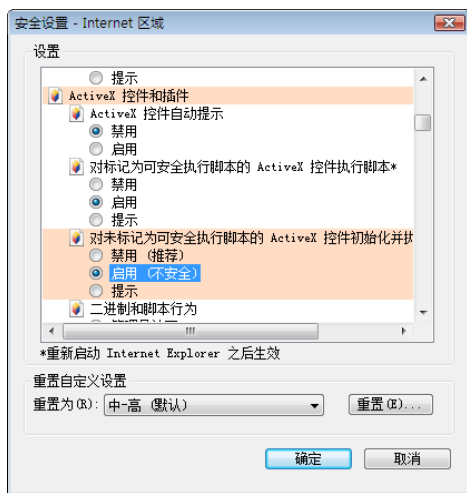


图 12-20 “安全设置 – Internet 区域”对话框



如果未在 IE 浏览器的安全设置中启用这两项，则在申请证书时会显示如图 12-21 所示的提示框。

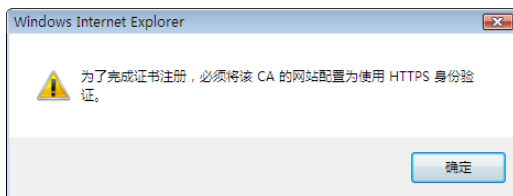


图 12-21 提示框

③ 单击“确定”按钮保存设置。

2. 信任证书颁发机构

如果客户端没有加入域，则必须配置为信任证书颁发机构，才能安装从证书服务器申请的证书。否则将无法安装。

① 打开 Web 浏览器，在地址栏中输入证书服务器的证书申请地址，格式为“http://证书服务器的 IP 地址/certsrv”。例如，http://192.168.1.10/certsrv。按回车键，显示如图 12-22 所示的“连接到”登录框。

② 在“用户名”和“密码”文本框中分别键入具有登录证书服务器权限的用户名和密码，单击“确定”按钮，显示如图 12-23 所示的“Active Directory 证书服务”窗口。

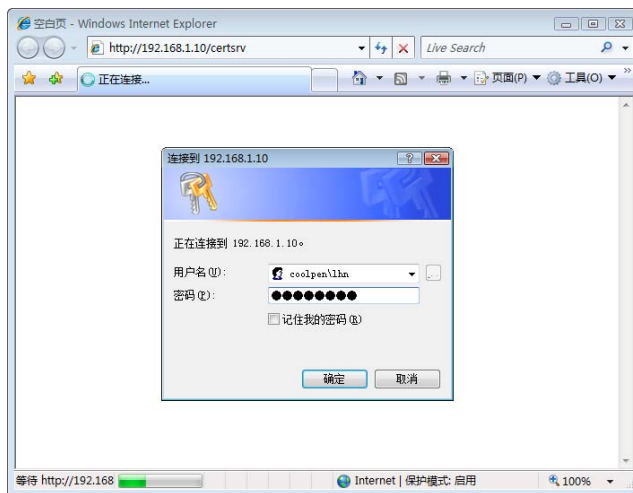


图 12-22 登录框

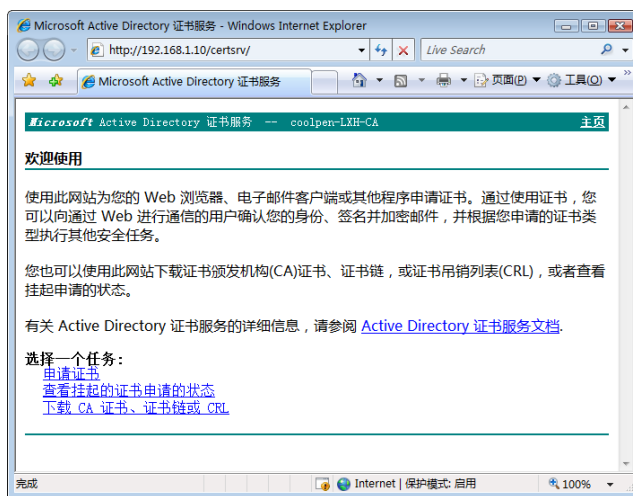


图 12-23 “Active Directory 证书服务”窗口

③ 单击“下载 CA 证书、证书链或 CRL”超级链接，显示如图 12-24 所示的“下载 CA 证书、证书链或 CRL”窗口，在其中下载证书或证书链。

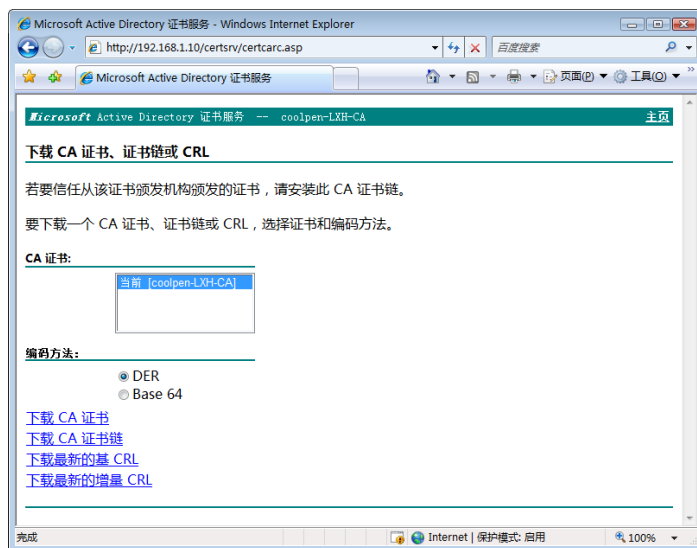


图 12-24 “下载 CA 证书、证书链或 CRL”窗口

④ 单击“下载 CA 证书”超级链接，显示如图 12-25 所示的“文件下载”对话框。单击“保存”按钮，将该证书保存到本地计算机中。

⑤ 证书下载完成以后，在 Windows 资源管理器中选择下载的证书链文件，右击并选择快捷菜单中的“安装证书”选项。显示“证书导入向导”对话框，如图 12-26 所示。

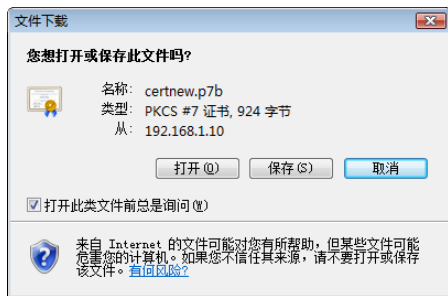


图 12-25 “文件下载”对话框



图 12-26 “证书导入向导”对话框

⑥ 单击“下一步”按钮，显示如图 12-27 所示的“证书存储”对话框，在其中选择保存证书的系统区域。

⑦ 选择“将所有证书放入下列存储”单选按钮，单击“浏览”按钮，显示如图 12-28 所示的“选择证书存储”对话框。选择“受信任的证书颁发机构”选项，然后单击“确定”按钮。

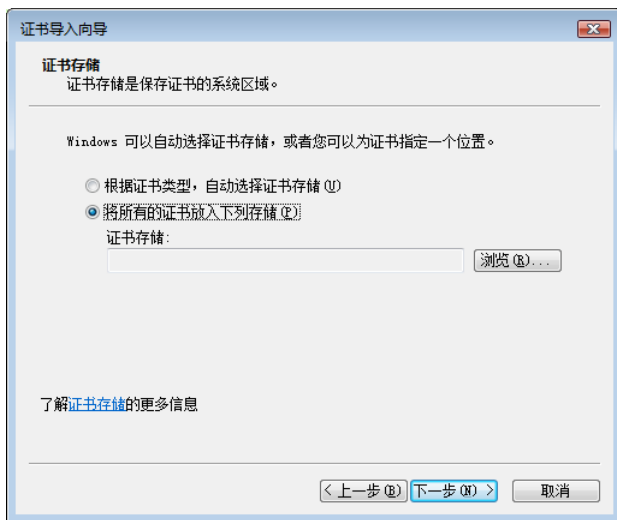


图 12-27 “证书存储”对话框

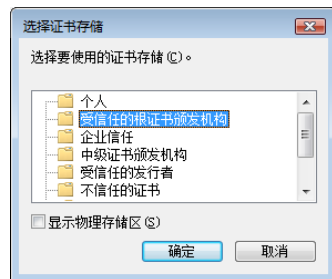


图 12-28 “选择证书存储”对话框

⑧ 单击“下一步”按钮，显示如图 12-29 所示的“正在完成证书导入向导”对话框。

⑨ 单击“完成”按钮，显示如图 12-30 所示的“安全性警告”对话框，要求确认是否安装此证书。

⑩ 单击“是”按钮，显示如图 12-31 所示的提示框。提示证书导入成功，此时可以颁发并安装证书。

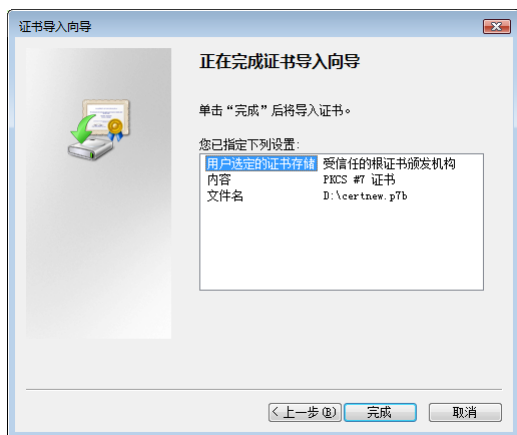


图 12-29 “正在完成证书导入向导”对话框

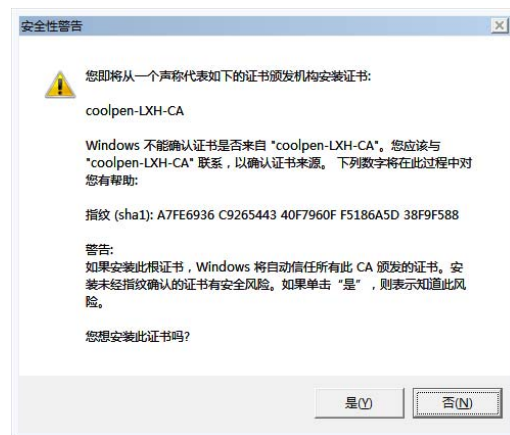


图 12-30 “安全性警告”对话框

3. 申请证书

① 登录到“Active Directory 证书服务”窗口，在“欢迎使用”窗口中单击“申请证书”超级链接，显示如图 12-32 所示的“申请一个证书”窗口。

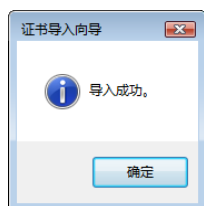


图 12-31 提示框

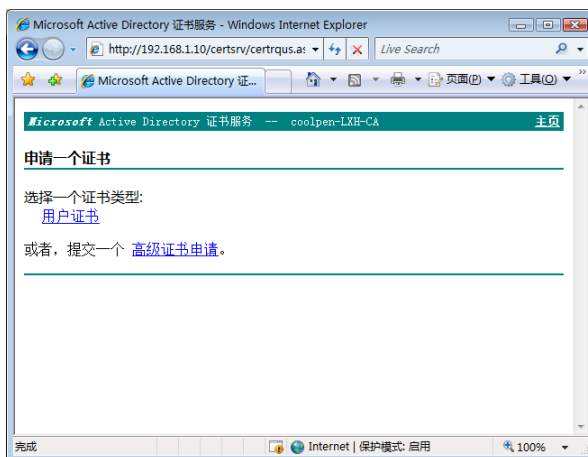


图 12-32 “申请一个证书”窗口

② 单击“用户证书”链接，显示如图 12-33 所示的“用户证书 - 识别信息”窗口。

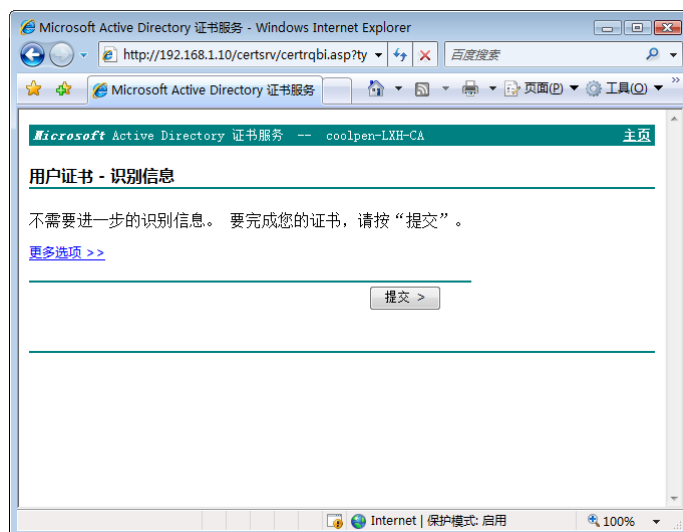


图 12-33 “用户证书 - 识别信息”窗口

③ 单击“提交”按钮，向证书服务器申请证书。完成后显示如图 12-34 所示的“证书已颁发”窗口，提示所申请的证书已颁发。

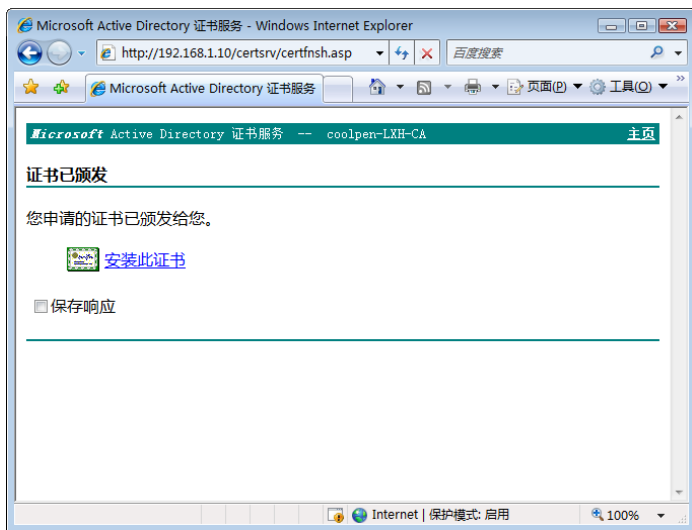


图 12-34 “证书已颁发”窗口

④ 单击“安装此证书”超级链接，显示如图 12-35 所示的“证书已安装”窗口，提示证书已经安装。

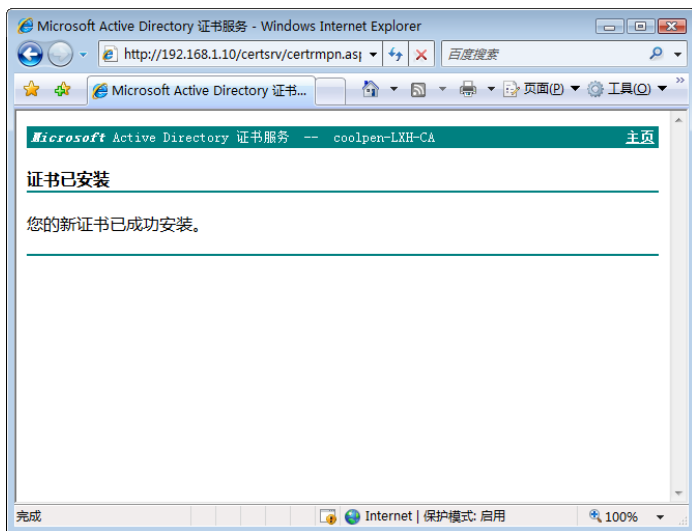


图 12-35 “证书已安装”窗口

12.3.2 使用“证书申请向导”申请证书

要使用“证书申请向导”向企业根 CA 申请证书，客户端计算机必须先加入域，并且使用域用户登录到域。这里以 Windows Vista 为例，介绍如何申请证书。

- ① 使用域用户账户登录到 Windows Vista 系统。
- ② 打开“开始”菜单，在“开始搜索”文本框中输入 mmc 命令。按回车键，打开“控制台 1”窗口，如图 12-36 所示。
- ③ 单击“文件”→“添加/删除管理单元”选项，显示如图 12-37 所示的“添加或删除管理单元”对话框。在“可用的管理单元”下拉列表框中选择“证书”选项，单击“添加”按钮添加到右侧“所选管理单元”列表框中。

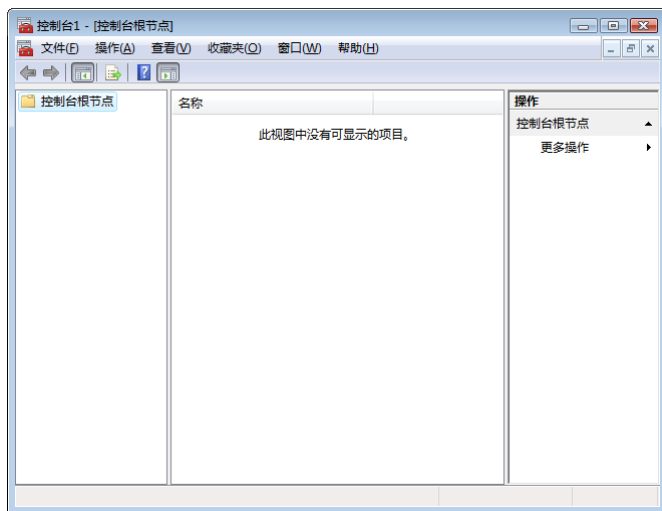


图 12-36 “控制台 1” 窗口

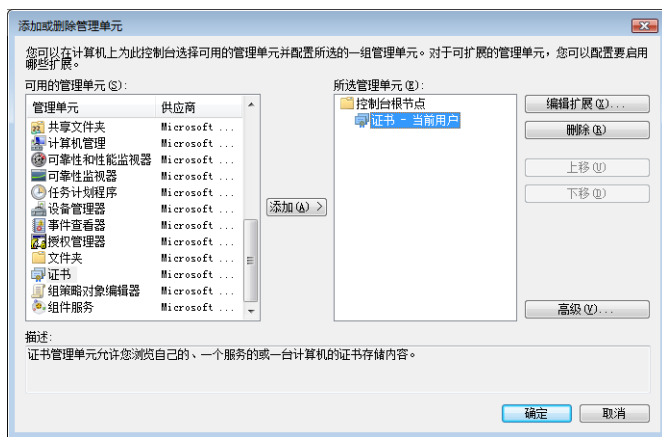


图 12-37 “添加或删除管理单元” 对话框

- ④ 单击“确定”按钮，将证书管理单元添加到控制台中，如图 12-38 所示。

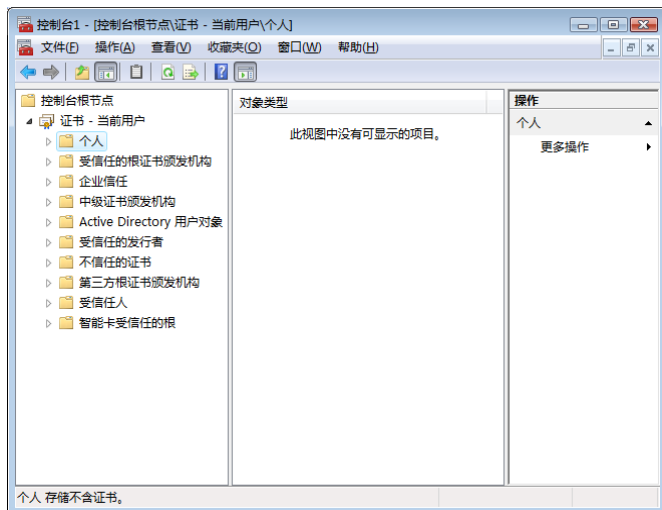


图 12-38 添加证书到控制台中

- ⑤ 展开“证书 - 当前用户”选项，选择“个人”选项。右击并选择快捷菜单中的“所有任务”→“申请新证书”选项，打开“证书注册”对话框，如图 12-39 所示。

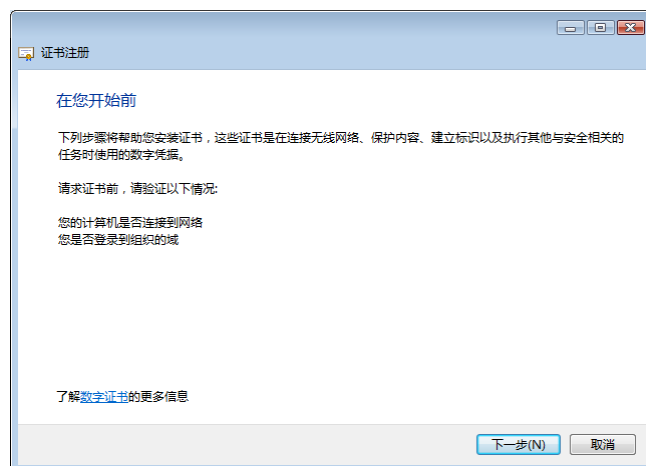


图 12-39 “证书注册”对话框

⑥ 单击“下一步”按钮，显示如图 12-40 所示的“申请证书”对话框。在列表框中选择待申请的证书类型，单击“详细信息”按钮可以查看该证书的详细信息。默认情况下，只列出可用的证书模板。

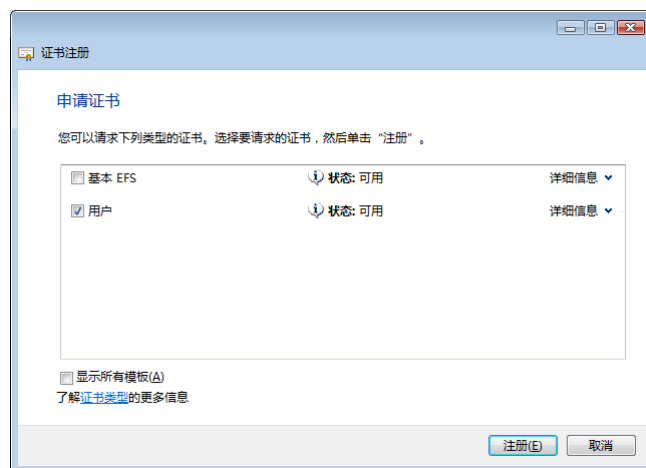


图 12-40 “申请证书”对话框

⑦ 单击“注册”按钮，系统会向证书服务器申请注册并自动安装，显示如图 12-41 所示的“证书安装结果”对话框。



图 12-41 “证书安装结果”对话框

⑧ 单击“完成”按钮关闭证书注册向导，并返回控制台。依次展开“证书 - 当前用户”→“个人”→“证书”选项，即可看到已注册成功的证书，如图 12-42 所示。

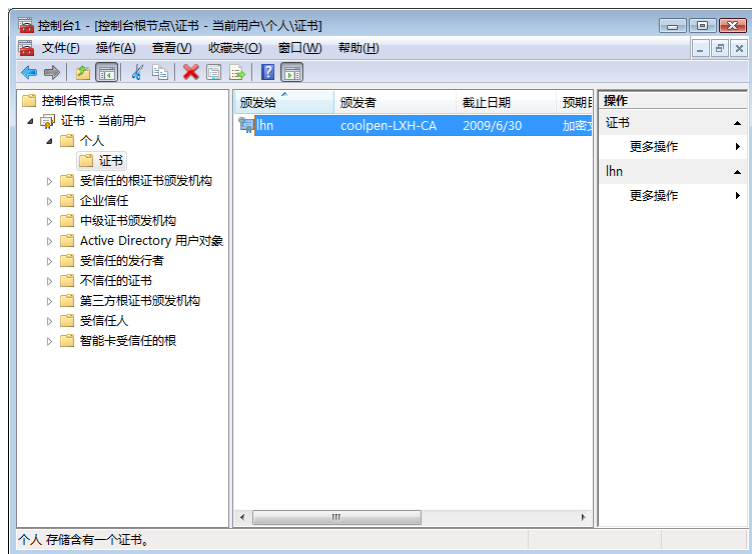


图 12-42 注册成功的证书

至此，证书注册完成。返回 Windows Server 2008 证书服务器，单击“开始”→“管理工具”→“Certification Authority”选项，打开“证书颁发机构”窗口。选择“颁发的证书”选项，即可看到所有已颁发的证书，如图 12-43 所示。



图 12-43 已颁发的证书

12.3.3 导出与导入证书

为了防止因意外故障或者重新安装系统而造成证书损坏或丢失，用户可以将证书导出以备份。当需要还原时，只需将证书导入即可，不必重新申请。

1. 导出证书

① 在客户端运行“mmc”命令，打开如图 12-44 所示的“控制台 1”窗口，添加“证书”管理单元。

② 展开要备份的证书所在的位置，例如“证书 - 当前用户”→“个人”→“证书”。选择要导出的证书，右击并选择快捷菜单中的“所有任务”→“导出”选项。打开“证书导出向导”对话框，如图 12-45 所示。

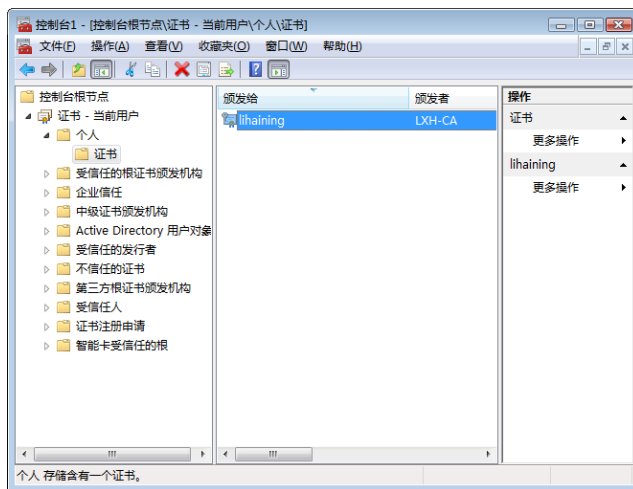


图 12-44 “控制台 1” 窗口

- ③ 单击“下一步”按钮，显示如图 12-46 所示的“导出私钥”对话框，选择是否导出私钥。



图 12-45 “证书导出向导” 对话框

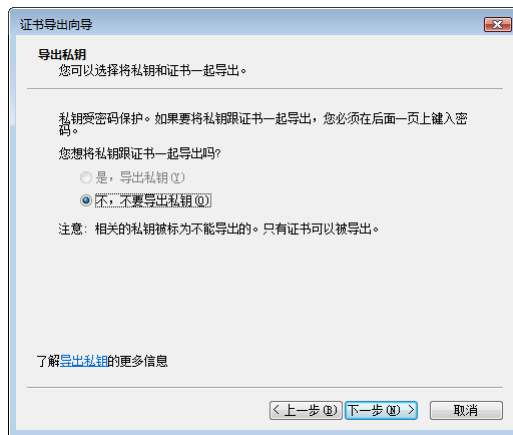


图 12-46 “导出私钥” 对话框

- ④ 单击“下一步”按钮，显示如图 12-47 所示的“导出文件格式”对话框，选择证书的导出格式。

- ⑤ 单击“下一步”按钮，显示如图 12-48 所示的“要导出的文件”对话框，在“文件名”文本框中键入证书的保存路径及文件名。

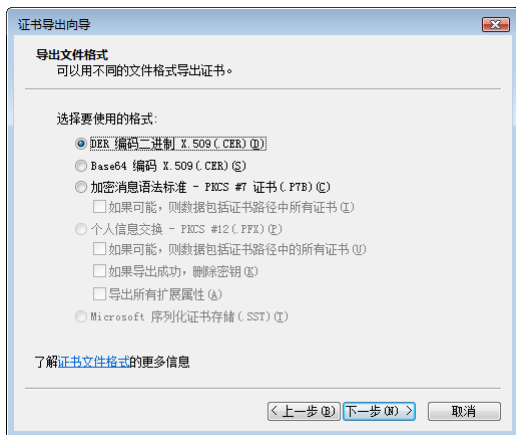


图 12-47 “导出文件格式” 对话框

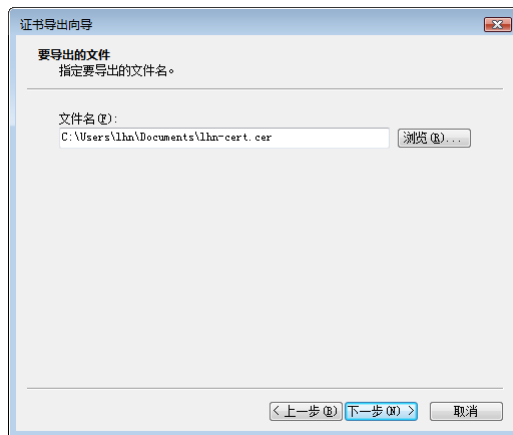


图 12-48 “要导出的文件” 对话框

- ⑥ 单击“下一步”按钮，显示如图 12-49 所示的“正在完成证书导出向导”对话框。

- ⑦ 单击“完成”按钮，显示如图 12-50 所示的提示框。提示证书导出完成，单击“确定”按钮。

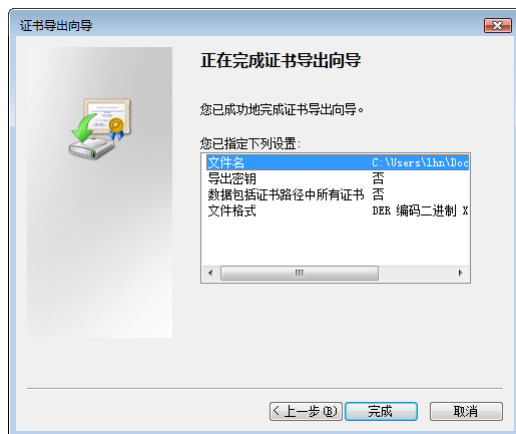


图 12-49 正在完成证书导出向导

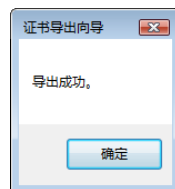


图 12-50 提示框

2. 导入证书

① 打开“控制台”窗口，添加“证书”管理单元。展开“个人”选项，右击“证书”选项选择快捷菜单中的“所有任务”→“导入”选项。打开“证书导入向导”对话框，如图 12-51 所示。

② 单击“下一步”按钮，显示如图 12-52 所示的“要导入的文件”对话框。单击“浏览”按钮，选择以前导出的证书文件。



图 12-51 “证书导入向导”对话框



图 12-52 “要导入的文件”对话框

- ③ 单击“下一步”按钮，显示如图 12-53 所示的“证书存储”对话框，选择证书的存储位置。

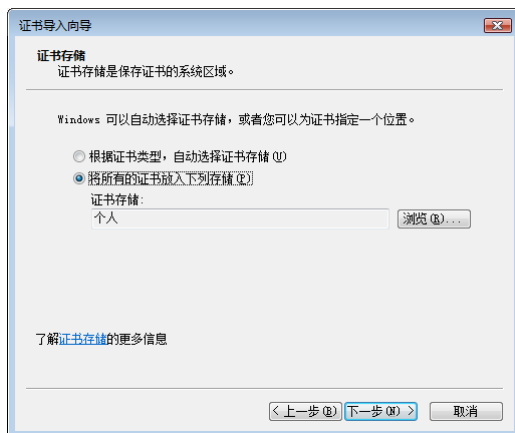


图 12-53 “证书存储”对话框

④ 单击“下一步”按钮，显示如图 12-54 所示的“正在完成证书导入向导”对话框，其中列出前面所做的配置。

⑤ 单击“完成”按钮，证书导入成功。显示如图 12-55 所示的提示框，单击“确定”按钮。

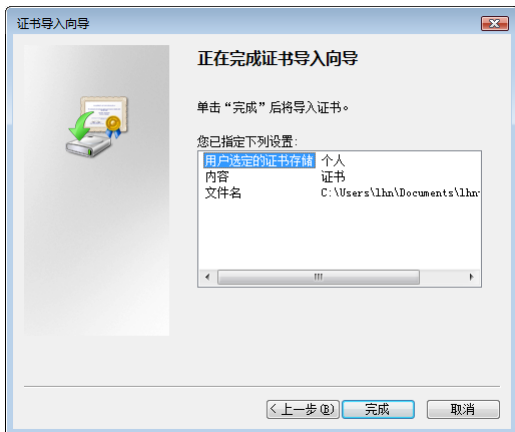


图 12-54 “正在完成证书导入向导”对话框



图 12-55 提示框

12.4 使用独立证书服务

独立证书服务器由于没有加入域，因此不能使用“证书申请向导”来申请，只能以 Web 方式向证书服务器申请证书。为了证书服务的安全，当用户申请证书后并不会立即安装，必须由管理员颁发后才能使用。

12.4.1 申请证书

在向服务器申请证书时，必须首先做好如下准备工作。

- (1) 在 IE 浏览器的安全设置中，将“对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本（不安全）”和“允许运行以前未使用的 ActiveX 控件而不提示”均选择为“启用（不安全）”选项。
- (2) 下载 CA 证书并导入到客户端上，使其信任证书颁发机构。

向独立服务器申请证书的操作步骤如下。

① 在 IE 浏览器中打开申请独立根证书的地址，格式为“http://证书服务器 IP 地址/certsrv”，显示的如图 12-56 所示的证书服务主页。

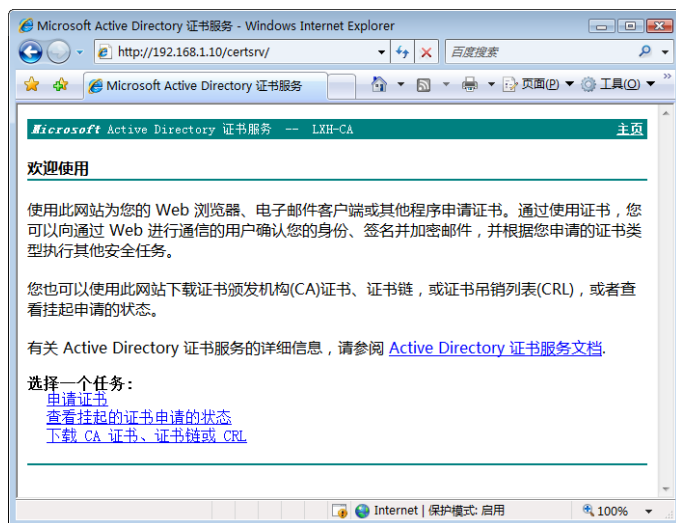


图 12-56 证书服务主页

② 单击“申请证书”超级链接，显示如图 12-57 所示的“申请一个证书”窗口。在其中可以直接申请 Web 浏览器证书或电子邮件证书，也可以提交高级证书申请。

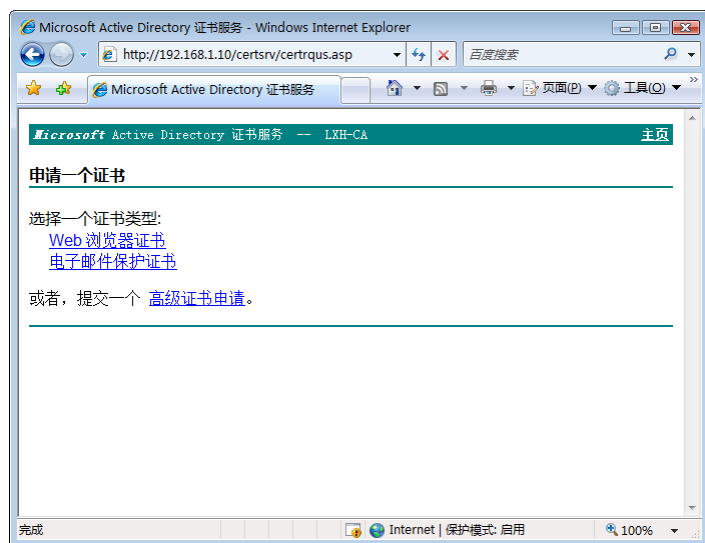


图 12-57 “申请一个证书”窗口

提示 如果要申请其他类型的证书，则单击“高级证书申请”超级链接。同时还可以选择不同的密钥类型，如图 12-58 所示。

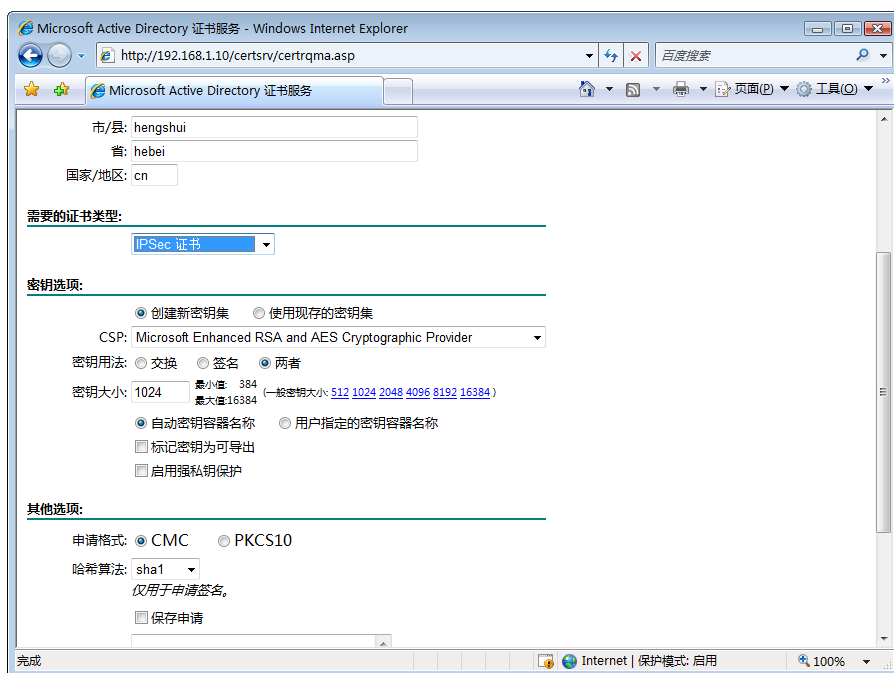


图 12-58 选择不同的密钥类型

③ 这里以申请电子邮件保护证书为例，单击“电子邮件保护证书”超级链接，显示如图 12-59 所示的“电子邮件保护证书 - 识别信息”窗口，输入电子邮件保护证书的识别信息即可。

提示 如果不想使用默认的密钥类型，可以单击“更多选项”链接。然后在显示页面中的“选择一个加密服务提供程序”下拉列表框中选择不同的密钥程序，如图 12-60 所示。



图 12-59 申请电子邮件证书



图 12-60 选择不同的密钥程序

④ 单击“提交”按钮，开始向证书服务器发送请求，并显示如图 12-61 所示的“证书正在挂起”窗口。提示已发出申请，但必须等待管理员来颁发证书。

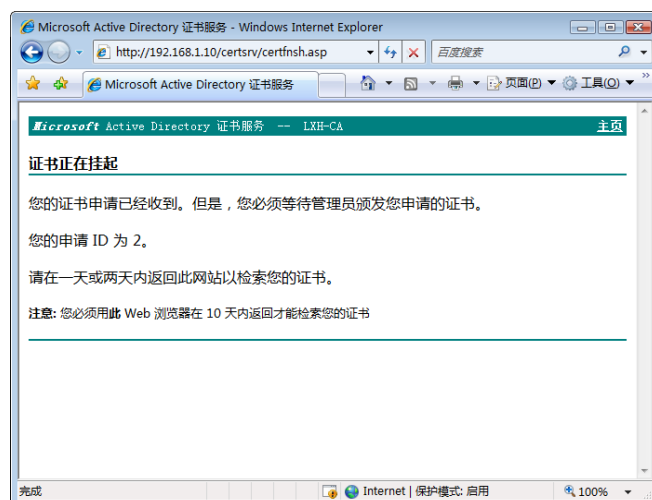


图 12-61 “证书正在挂起”窗口

12.4.2 颁发证书

此时，在 Windows Server 2008 服务器上，需要由管理员查看证书申请，并颁发证书。

① 登录到证书服务器，单击“开始”→“管理工具”→“Certification Authority”选项，打开“certsrv”窗口。在左侧栏中选择“挂起的申请”选项，显示所有提交的证书申请，如图 12-62 所示。



图 12-62 所有提交的证书申请

② 选择要颁发的证书，右击并选择快捷菜单中的“所有任务”→“颁发”选项，即可颁发该证书。同时已颁发的证书将会自动转到“颁发的证书”窗口中，如图 12-63 所示。

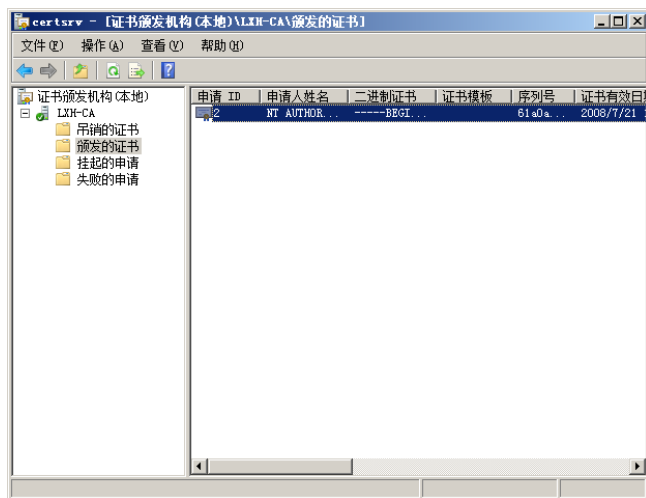


图 12-63 已颁发的证书

此时证书颁发完成，在客户端上可以安装或下载证书。

12.4.3 在客户端安装证书

在客户端安装证书的操作步骤如下。

① 在客户端重新打开证书服务主页，单击“查看挂起的证书申请的状态”超级链接。显示如图 12-64 所示的“查看挂起的证书申请的状态”窗口，其中列出曾经申请的证书。

② 单击证书名称，例如“电子邮件保护证书”。显示如图 12-65 所示的“证书已颁发”窗口，提示该证书已颁发，可以安装。

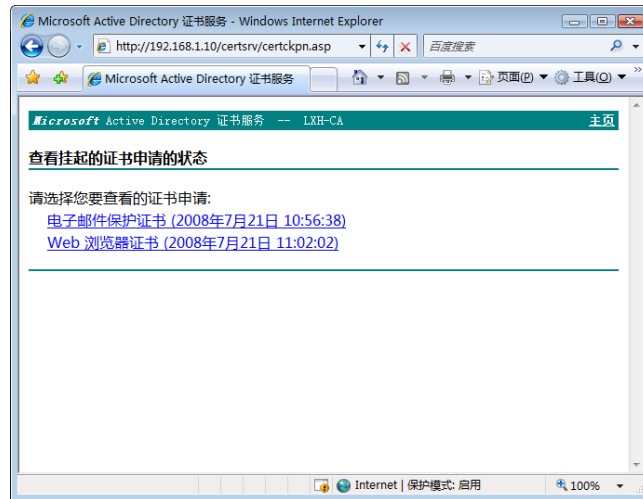


图 12-64 “查看挂起的证书申请的状态”窗口

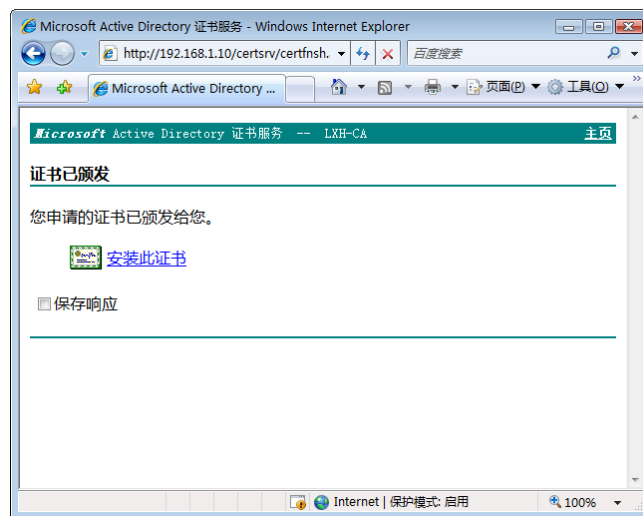


图 12-65 “证书已颁发”窗口

③ 单击“安装此证书”链接，显示如图 12-66 所示的“证书已安装”窗口，即可将该证书安装在本地计算机上。

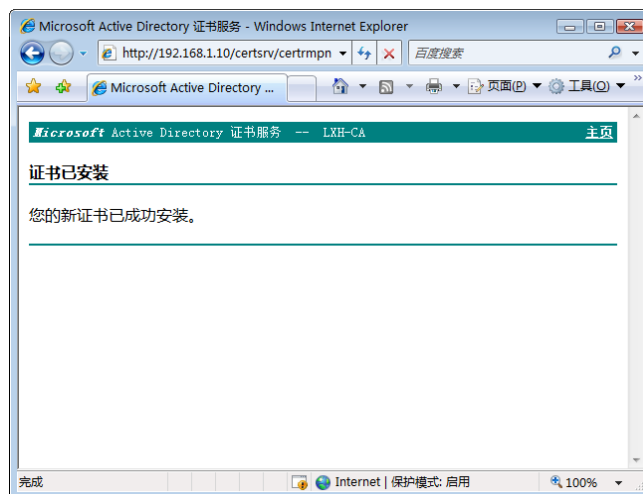


图 12-66 “证书已安装”窗口

12.5 备份与还原证书服务器

为了防止证书服务器因意外故障或被误删而导致证书丢失，从而造成用户的损失。管理员和用户均应定期备份证书服务器中的证书，以在证书丢失或损坏时能够及时还原，可继续使用而不必重新申请。

12.5.1 备份证书

备份证书的操作步骤如下。

① 以管理员用户身份登录到证书服务器，打开“证书颁发机构”窗口。右击证书服务器名称，选择快捷菜单中的“所有任务”→“备份 CA”选项。打开“证书颁发机构备份向导”对话框，如图 12-67 所示。

② 单击“下一步”按钮，显示如图 12-68 所示的“要备份的项目”对话框。在“选择要备份的项目”选项组中选择要备份的组件，如“私钥和 CA 证书”及“证书数据库和证书数据库日志”；在“备份到这个位置”文本框中键入备份证书的保存路径或单击“浏览”按钮选择。

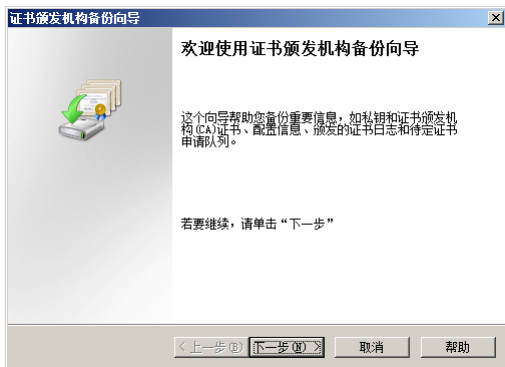


图 12-67 “证书颁发机构备份向导”对话框

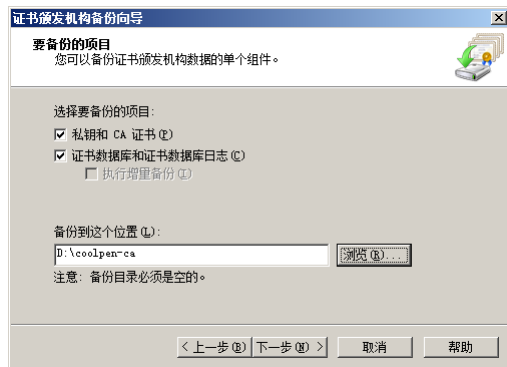


图 12-68 “要备份的项目”对话框

③ 单击“下一步”按钮，显示如图 12-69 所示的“选择密码”对话框。为安全起见，可在“密码”文本框中设置访问 CA 证书文件的密钥，防止被他人访问。

④ 单击“下一步”按钮，显示如图 12-70 所示的“正在完成证书颁发机构备份向导”对话框。

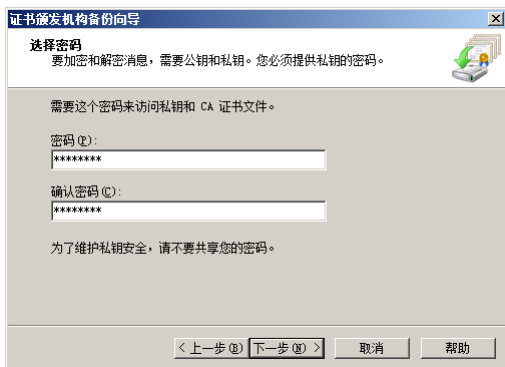


图 12-69 “选择密码”对话框

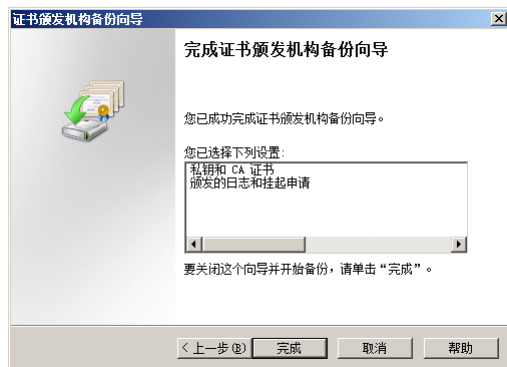


图 12-70 “正在完成证书颁发机构备份向导”对话框

⑤ 单击“完成”按钮，即可备份证书。

12.5.2 还原证书

还原证书的操作步骤如下。

① 在“证书颁发机构”窗口中右击证书服务器名，选择快捷菜单中的“所有任务”→“还原 CA”

选项，显示如图 12-71 所示的提示框。提示还原证书过程中不能运行 Active Directory 证书服务，需要立即将其停止。

② 单击“确定”按钮，停止 Active Directory 证书服务。启动证书颁发机构还原向导，如图 12-72 所示。



图 12-71 提示框

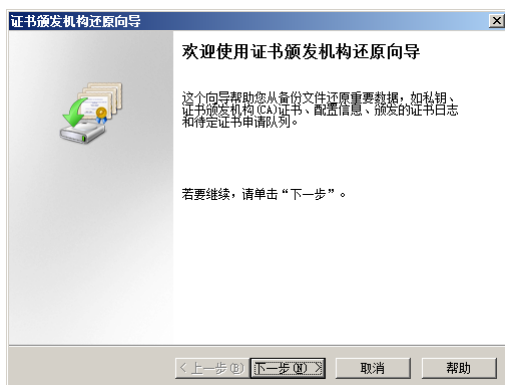


图 12-72 证书颁发机构还原向导

③ 单击“下一步”按钮，显示如图 12-73 所示的“要还原的项目”对话框。在“选择要还原的项目”选项组中选择要还原的选项，在“从这个位置还原”文本框中输入备份证书所在的路径或者单击“浏览”按钮选择。

④ 单击“下一步”按钮，显示如图 12-74 所示的“提供密码”对话框，在“密码”文本框中输入备份 CA 时设置的密码。

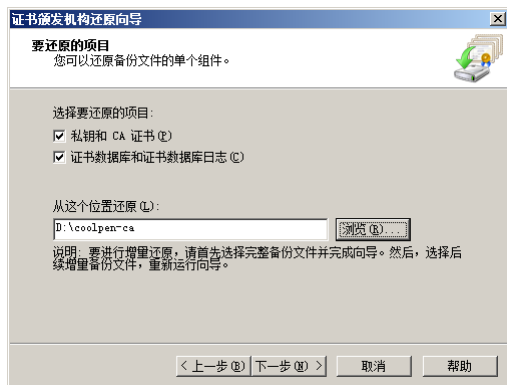


图 12-73 “要还原的项目”对话框

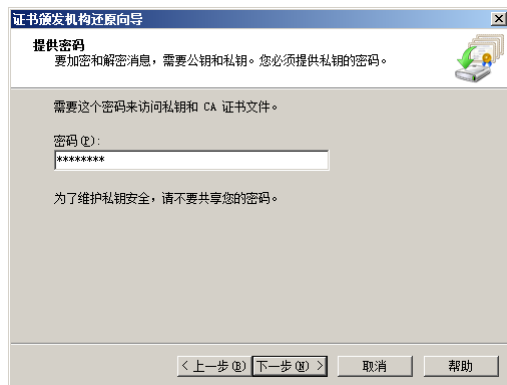


图 12-74 “提供密码”对话框

⑤ 单击“下一步”按钮，显示如图 12-75 所示的“完成证书颁发机构还原向导”对话框。

⑥ 单击“完成”按钮，证书还原成功。显示如图 12-76 所示的提示框，提示是否要启动服务。



图 12-75 “完成证书颁发机构还原向导”对话框



图 12-76 提示框

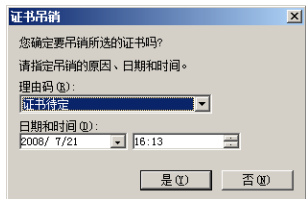
⑦ 单击“是”按钮，启动 Active Directory 证书服务。

12.6 管理证书服务

在企业中，当员工辞职或调到其他部门后原来申请的证书将不再使用，此时网络管理员应及时吊销其证书。而证书都有一定的有效期限，为了保证在有效期过后仍能继续使用，应及时更新或者续订。

12.6.1 吊销证书

如果某些证书不再使用，即可将其吊销。不过，吊销证书只能在证书服务器上完成。



(1) 登录到证书服务器，打开“证书颁发机构”控制台。在“颁发的证书”窗口中选择待吊销的证书，右击并依次选择快捷菜单中的“所有任务”→“吊销证书”选项。显示如图 12-77 所示的“证书吊销”对话框，在“理由码”下拉列表框中选择吊销的原因。

(2) 单击“是”按钮，即可吊销该证书。当证书被吊销以后将显示在“吊销的证书”窗口中，如图 12-78 所示。

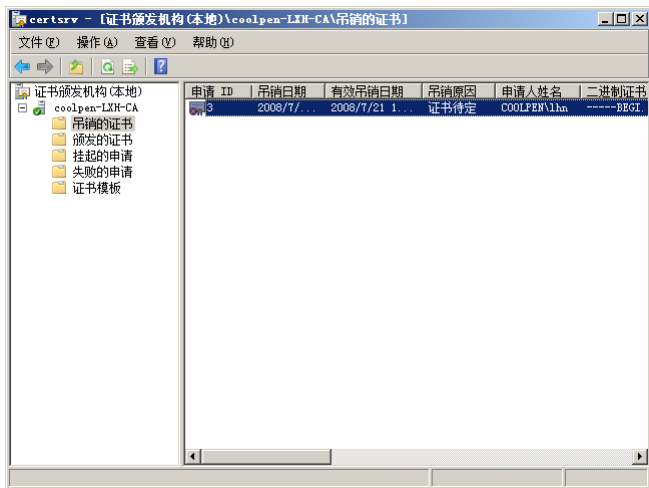


图 12-78 “吊销的证书”窗口

12.6.2 解除吊销的证书

如果有些已吊销的证书需要继续使用，则可以解除吊销。不过需要注意的是，只有吊销原因为“证书待定”的证书才能解除吊销，其他原因吊销的证书将不能解除。

在“吊销的证书”窗口中选择要解除吊销的证书，右击并选择快捷菜单中的“所有任务”→“解除吊销证书”选项即可。

如果证书不能被解除吊销，将显示如图 12-79 所示的提示框，提示取消吊销失败。

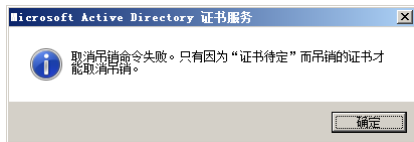


图 12-79 提示框

12.6.3 证书续订

证书都有一定的有效期限，当有效期过后证书将会无效。因此若要继续使用证书，必须在证书到期前更新或者续订，不过只有登录到域以后才有权续订证书。

1. 用新密钥续订证书

① 在客户端运行“mmc”命令打开“控制台”窗口，添加“证书”管理单元。

② 依次展开“个人”→“证书”选项，选择待续订的证书。右击并选择快捷菜单中的“所有任务”→“用新密钥续订证书”选项，打开“证书注册”对话框，如图 12-80 所示。

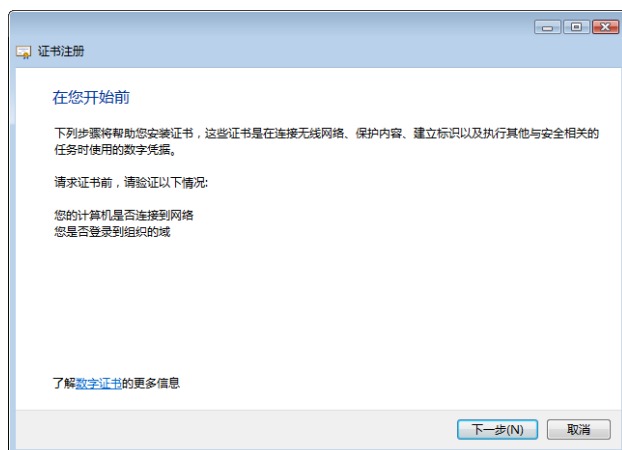


图 12-80 “证书注册”对话框

③ 单击“下一步”按钮，显示如图 12-81 所示的“申请证书”对话框。其中列出可以请求的证书，单击“详细信息”按钮可以查看该证书的详细信息。



图 12-81 “申请证书”对话框

④ 单击“注册”按钮，开始注册证书服务器。完成后显示如图 12-82 所示的“证书安装结果”对话框，提示注册成功。



图 12-82 “证书安装结果”对话框

⑤ 单击“完成”按钮，证书申请成功。

2. 用相同密钥续订证书

① 打开“证书”管理单元，选择待续订的证书。右击并选择快捷菜单中的“所有任务”→“高级操作”→“使用相同密钥续订此证书”选项，运行证书注册向导。

② 单击“下一步”按钮，显示如图 12-83 所示的“申请证书”对话框，其中列出要请求的证书。



图 12-83 “申请证书”对话框

③ 单击“注册”按钮，开始注册证书服务器。完成后显示如图 12-84 所示的“证书安装结果”对话框，单击“完成”按钮即可。

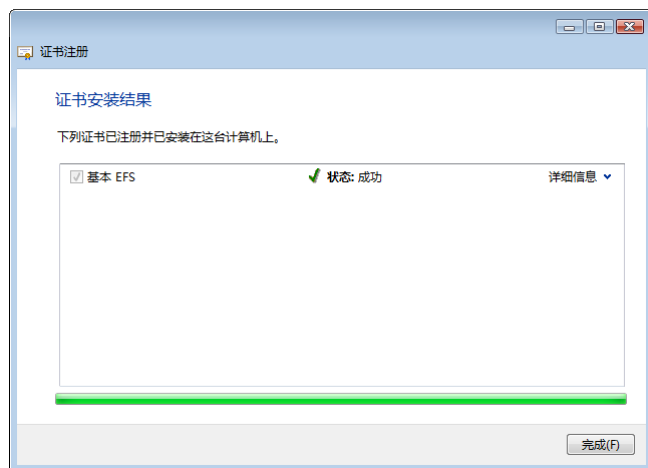


图 12-84 “证书安装结果”对话框

12.7 配置安全 Web 服务器

为了保证数据传输过程中的安全，很多 Web 网站都配置 SSL 安全设置，即 HTTPS 网站。不过 SSL 网站必须使用证书，如果企业中部署了证书服务器，即可为 Web 服务器申请证书并配置。

12.7.1 为 Web 服务器申请证书

为 Web 服务器申请证书有两种方式，一是利用 IE 浏览器；二是在 IIS 管理器中利用“创建域证书”来申请。另外，如果是在其他计算机上申请的证书，也可以复制到 Web 服务器中，然后在 IIS 管理器中导入。

1. 利用 IE 浏览器申请

- ① 登录到 Web 服务器，在 IE 浏览器中打开证书服务器的证书服务主页，如图 12-85 所示。



图 12-85 证书服务器的证书服务主页

- ② 单击“申请证书”超级链接，显示如图 12-86 所示的“申请一个证书”窗口。

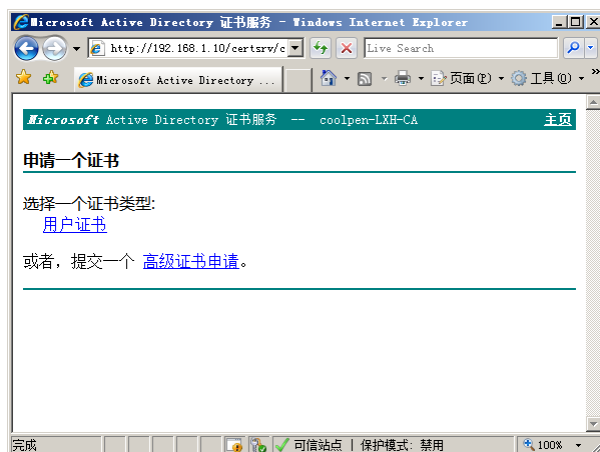


图 12-86 “申请一个证书”窗口

- ③ 单击“高级证书申请”链接，显示如图 12-87 所示的“高级证书申请”窗口。

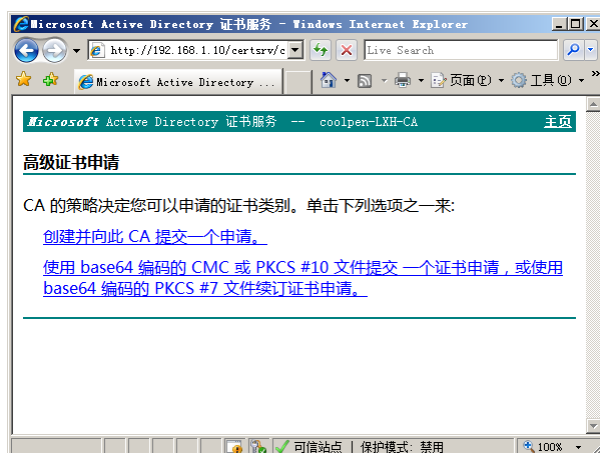


图 12-87 “高级证书申请”窗口

④ 单击“创建并向此 CA 提交一个申请”超级链接，显示如图 12-88 所示的申请 Web 证书窗口。在“证书模板”下拉列表框中选择“Web 服务器”选项，输入识别信息并设置密钥。

图 12-88 申请 Web 证书窗口

⑤ 单击“提交”按钮，向证书服务器提交申请。完成后显示如图 12-89 所示的“证书已颁发”窗口，提示所申请的证书已颁发。

图 12-89 “证书已颁发”窗口

⑥ 单击“安装此证书”超级链接，即可成功安装此证书，显示如图 12-90 所示的“证书已安装”窗口。

提示 如果 Web 服务器没有加入域，则必须首先配置信任证书颁发机构。并且所申请的证书必须由管理员颁发后才能安装。

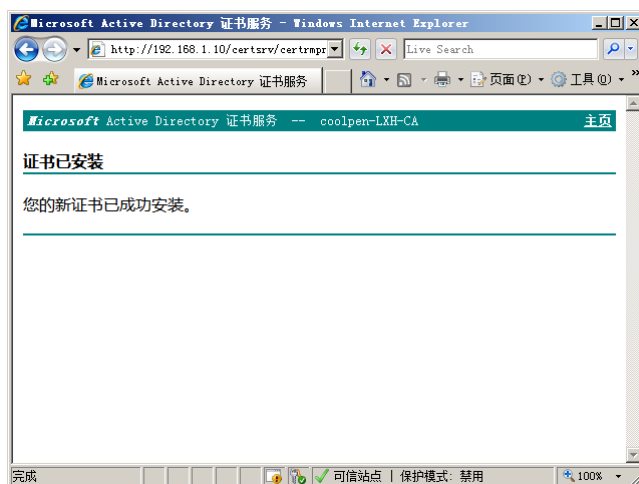


图 12-90 “证书已安装”窗口

2. 创建域证书

① 单击“开始”→“管理工具”→“Internet 信息服务 (IIS)”选项，选择 Web 服务器名称。在“主页”窗口中双击“服务器证书”图标，显示如图 12-91 所示的“服务器证书”窗口。



图 12-91 “服务器证书”窗口

② 单击“操作”窗格中的“创建域证书”超级链接，显示如图 12-92 所示的“可分辨名称属性”对话框，输入名称、组织及省/市等信息。

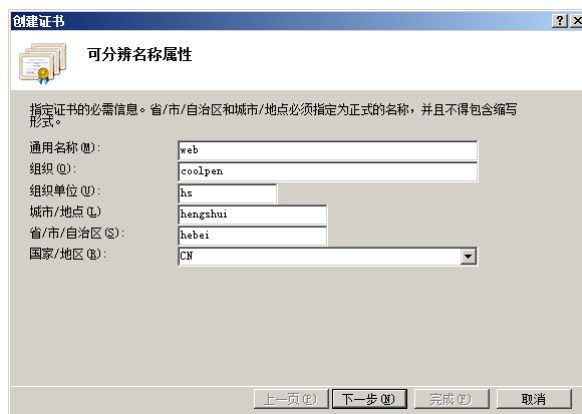


图 12-92 “可分辨名称属性”对话框

③ 单击“下一步”按钮，显示如图 12-93 所示的“联机证书颁发机构”对话框。

④ 单击“浏览”按钮，显示如图 12-94 所示的“选择证书颁发机构”对话框，在列表框中选择证书颁发机构。

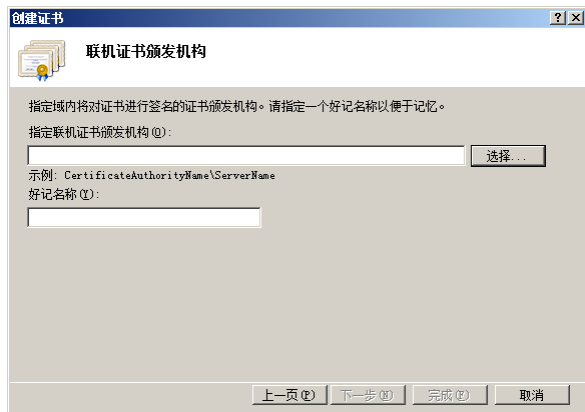


图 12-93 “联机证书颁发机构”对话框

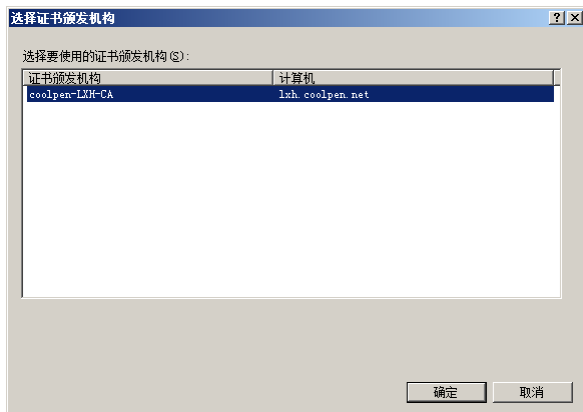


图 12-94 “选择证书颁发机构”对话框

⑤ 单击“确定”按钮，返回如图 12-95 所示的“联机证书颁发机构”对话框，在“好记名称”文本框中输入一个名称。



图 12-95 “联机证书颁发机构”对话框

⑥ 单击“完成”按钮，证书申请完成，返回到 IIS 管理器窗口。在“服务器证书”窗口中显示新创建的证书，如图 12-96 所示。

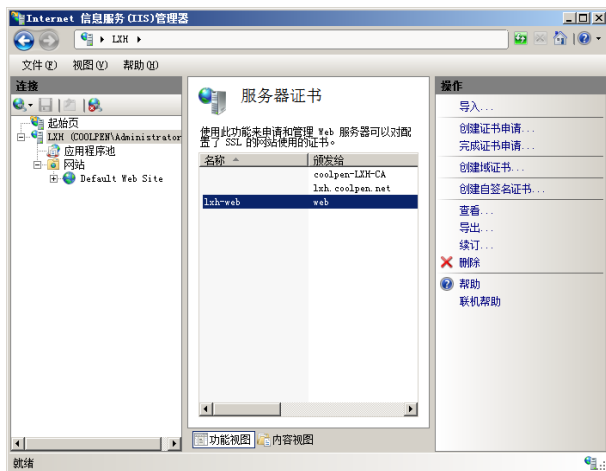


图 12-96 新创建的证书

12.7.2 将证书应用于 Web 服务器

将证书应用于 Web 服务器的操作步骤如下。

① 在 IIS 管理器窗口中右击“网站”选项，选择快捷菜单中的“添加网站”选项，显示如图 12-97 所示的“添加网站”对话框。

在其中设置如下选项。

网站名称：为 Web 网站键入一个名称。

物理路径：指定 Web 网站的主目录。

类型：选择“https”选项，创建一个 https 网站。

IP 地址和端口：指定一个 IP 地址，端口使用默认的 443 即可。

主机名：输入主机的名称。

添加的 https 网站如图 12-98 所示。

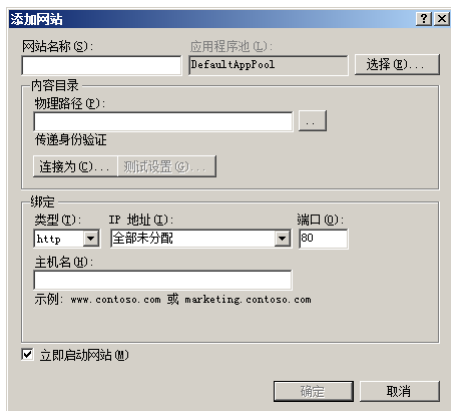


图 12-97 “添加网站”对话框

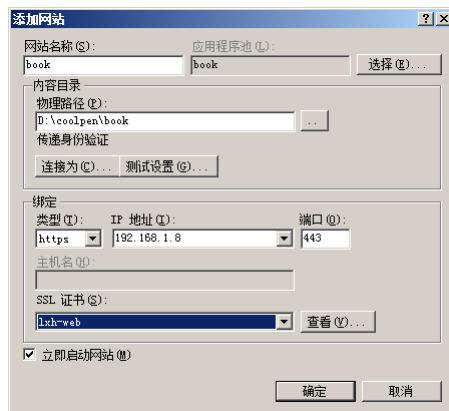


图 12-98 添加的 https 网站

② 单击“确定”按钮，完成新网站的创建，如图 12-99 所示。

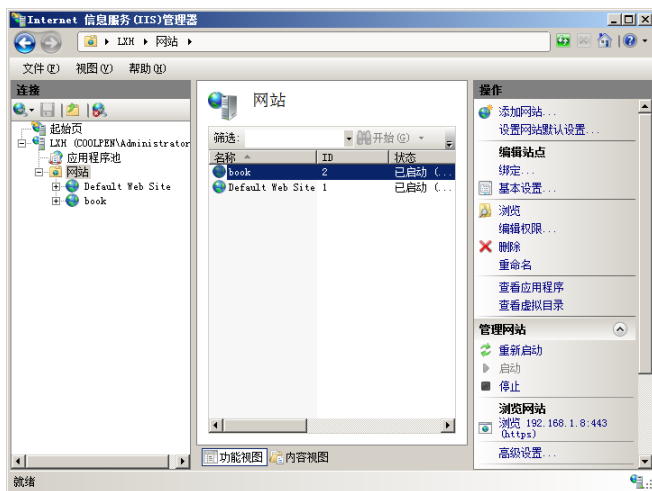


图 12-99 创建完成的新网站

至此，SSL 网站创建完成。

12.7.3 在工作站上验证 Web 服务器

如果客户端没有安装证书，那么当访问 Web 服务器时就会提示证书有问题。只有在安装证书以后，才能以加密方式浏览 Web 网站。

(1) 在客户端上打开 IE 浏览器，在地址栏中输入 Web 网站的地址，格式为“https://Web 网站地址”。按回车键，提示“此网站的安全证书有问题”，如图 12-100 所示。

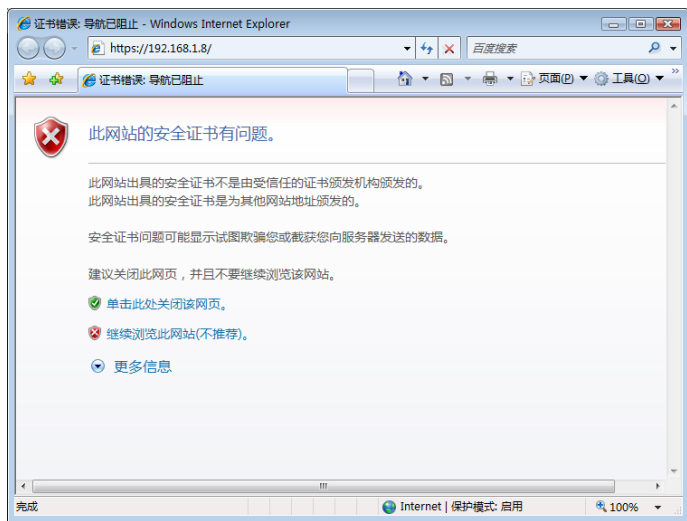


图 12-100 提示证书有问题

(2) 如果要继续浏览此网站，单击“继续浏览此网站（不推荐）”超级链接，显示如图 12-101 所示的窗口。同时，在地址栏中将显示“证书错误”。

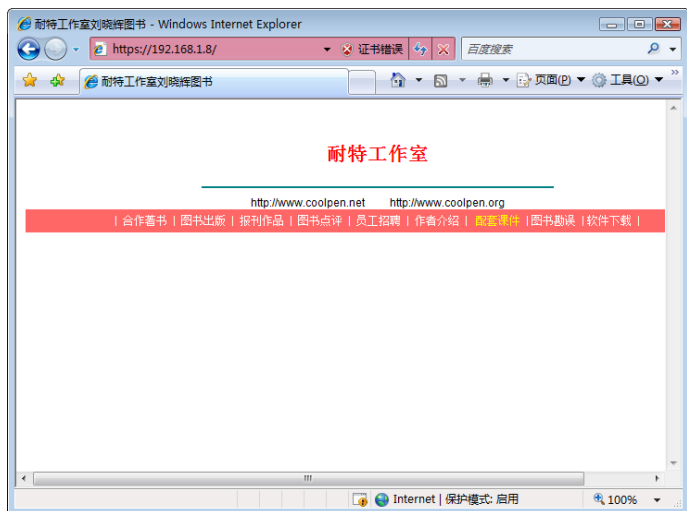


图 12-101 浏览 Web 网站

此时，向证书服务器申请一个证书，或者将证书服务器的证书复制到本地计算机并导入，即可使用安全 Web 方式连接到相应的站点。

12.8 Windows Server 2003/2008 的配置差异

在 Windows Server 2003 中，证书服务器的安装和配置方式均与 Windows Server 2008 不同，但客户端申请证书的方式相同。

打开“Windows 组件向导”对话框，选中“证书服务”复选框，如图 12-102 所示。单击“下一步”按钮，根据系统提示插入 Windows Server 2003 安装盘即可。

在安装证书服务过程中，可以选择企业根或独立根，如图 12-103 所示。同时，在安装过程中也可以设置证书加密方式、公用名称及有效日期等。

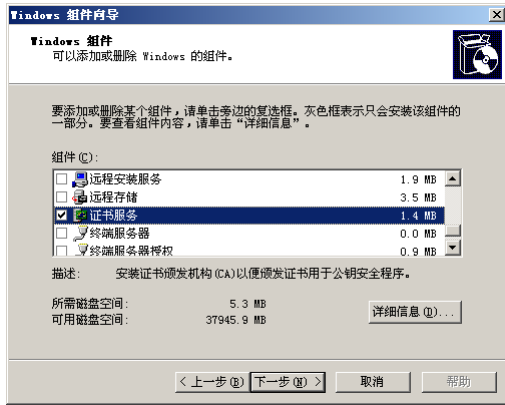


图 12-102 选中“证书服务”复选框

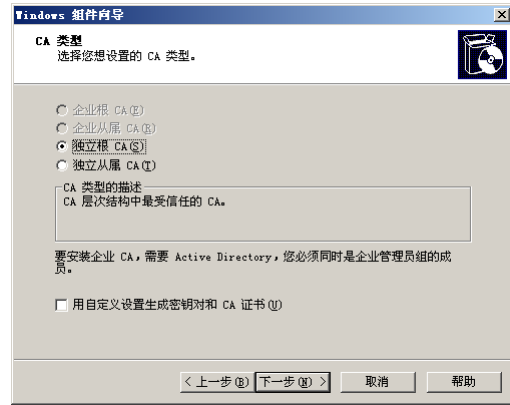


图 12-103 选择企业根或独立根

第 13 章 配置与管理终端服务

管理网络服务器是网络管理员必不可少的工作，传统的方式是实行面对面的管理。但对于规模较大且服务器数量较多，或者服务器距离较远的网络来说，这种方式是比较困难的。而利用 Windows 终端服务（Terminal Services, TS），即可在网络中的任何一台计算机上，借助于远程终端远程管理服务器。就像管理本地计算机一样可以执行各种操作并运行各种应用程序，这也是网络管理员最常用的管理方式。

13.1 安装终端服务

Windows Server 2008 集成了终端服务功能，不仅继承了早期 Windows 终端服务的所有优点，并且还提供了应用程序虚拟化功能，因此 Windows Server 2008 的终端服务被称为“桌面虚拟化”服务。其中包括两种类型的虚拟技术，一是虚拟服务器桌面，即传统的终端服务。客户端直接访问服务器桌面，并在服务器端运行应用软件；二是通过终端服务定制虚拟应用程序，客户端通过 RDP 链接文件或者 Web 访问方式访问终端服务器授权访问的应用程序，并在服务器端运行应用软件。客户端只是在屏幕上显示更新内容，允许通过键盘和鼠标交互。

13.1.1 终端服务概述

Windows Server 2008 系统中的终端服务无论是在功能、性能，以及用户体验方面都做了很大的改进。借助终端服务，管理员可以实现如下操作。

- （1）部署与用户的本地桌面集成的应用程序。
- （2）提供对集中式管理的 Windows 桌面的访问。
- （3）支持应用程序的远程访问。
- （4）保证数据中心内的应用程序和数据的安全。

与早期版本相比，Windows Server 2008 终端服务主要有以下几个方面的改进。

（1）TS RemoteApp

TS RemoteApp 程序通过终端服务就像在本地计算机上运行一样，并且可以与其本地程序一起运行 TS RemoteApp。如果用户在同一个终端服务器上运行多个 RemoteApp，则 RemoteApp 将共享同一个终端服务会话。另外，用户可以使用如下方法访问 TS RemoteApp。

使用管理员创建和分发的“开始”菜单或其桌面上的程序图标。

运行名称与 TS RemoteApp 关联的文件。

使用 TS Web Access 网站上的 TS RemoteApp 超级链接。

（2）TS 网关

TS 网关的作用是使得到授权的用户能够使用 Remote Desktop Connection (RDC) 6.0 连接到公司网络的终端服务器和远程桌面，该网关使用的是可以越过 HTTPS 的远程桌面协议 (RDP)，从而形成一条经过加密的安全连接。使用 TS 网关不需要配置虚拟专用网 (VPN) 连接即可使远程用户通过 Internet 连接到公司网络，从而提供一个全面安全的配置模型，通过该模型可以控制对特定资源的访问。TS 网关管理单元控制台采用的是一站式管理工具，使用该功能可以配置相应的用户策略，即配置用户连接到网络资源所需满足的条件。

(3) TS Web 访问

使用 TS Web 访问,能够使用户从 Web 浏览器使用 TS RemoteApp。TS Web 包含一个默认的网页,使用该网页,用户可以在 Web 上部署 TS RemoteApp。借助于 TS Web 访问,用户可以直接访问 Internet 或 Intranet 上的网站,以及可用的 TS RemoteApp 程序列表。当用户启动 TS RemoteApp 程序时,即可在该应用程序所在的终端服务器上启动一个终端服务会话。

(4) TS 会话代理

TS 会话代理是 Windows Server 2008 Release Candidate 中的一个新功能,它提供一个比用于 TS 的 Microsoft 网络负载均衡更简单的方案。借助 TS 会话代理功能,可以将新的会话分发到网络内负载最少的服务器,从而可以保证网络及服务器的性能。并且用户可以重新连接到现有会话,而不必知道有关建立会话的服务器的特定信息。使用该功能,管理员可以将每个终端服务器的 Internet 协议 (IP) 地址添加一条 DNS 条目。

提示



当网络中的一个服务器宕机时,用户的连接将会自动连接到网络内的下一个负载最少的服务器。

(5) TS 轻松打印

TS 轻松打印是 Windows Server 2008 Release Candidate 中的一个新功能,它能够使用户从 TS RemoteApp 程序或远程桌面会话安全可靠地使用客户端上的本地或网络打印机。当用户需要从 TS RemoteApp 程序或远程桌面会话中打印时,终端用户将会从本地客户端看到打印机用户界面,并且可以使用所有打印机功能。

13.1.2 虚拟化

Windows Server 2008 中增加了虚拟化功能,这是 Windows Server 2003 中所没有的。利用该功能只需在终端服务器安装并发布应用程序,在客户端上就可以使用。而且无需安装,从而降低成本,提高资源利用率。

1. 桌面虚拟化的优点

桌面虚拟化应用在客户端系统中仅需要安装操作系统即可,根据需要安装尽量少的应用程序。这样即可提高客户端的运行速度,也可以降低系统维护复杂程度。

部署桌面虚拟化具备以下优点。

(1) 减少管理桌面的时间:桌面虚拟化的最大好处是集中配置客户端需要的应用程序,网络管理员在服务器桌面,而不是每个用户的桌面管理众多的客户端。这样减少了现场支持工作,并且加强了对应用软件和补丁管理的控制。

(2) 更好地管理应用程序补丁:网络管理员只需在服务器上安装并调试应用程序更新,客户端即可使用新版本,从而降低了部署的时间、难度,以及工作强度。

(3) 降低应用程序和其他软件的冲突:客户端安装软件的不确定性将会增加部署应用程序和其他软件冲突的可能性,服务器端集中部署后业务的连续性和数据的安全性也得到了提高。

(4) 提升客户端的执行效率:客户端在系统启动时不需要加载其他 DLL 文件,所有的计算都是在服务器中完成。客户端仅显示结果或者提交数据,并不运行应用程序。应用程序可以使用客户端的本地资源,并没有永久性安装在客户端上带来的开销问题。

(5) 降低客户端硬件投资。

(6) 节省企业的空间、耗能和成本。

(7) 减少客户端的“宕机”次数:如果客户端的数据保存在服务器中,将加强用户数据安全性,同时提高系统的稳定性、可靠性及易操作性。

(8) 支持并发运行：虚拟化技术允许用户在台计算机上同时运行同一个应用程序，而每个用户数据只能自己访问，确保了数据的安全。

(9) 发布应用软件，而不是分发整个桌面环境：Windows Server 2008 可以将某个应用程序分发给某个用户，而不是分发给所有的用户。

(10) 发布应用程序 RDP 链接：Windows Server 2008 和 Windows Vista 操作系统不需要安装任何额外的应用程序，通过终端服务创建的 RDP 文件即可执行终端服务器上的应用程序。但 Windows XP/2003 需要安装 RDP 6.0 客户端补丁。

2. 桌面虚拟化的缺点

桌面虚拟化具备以下缺点。

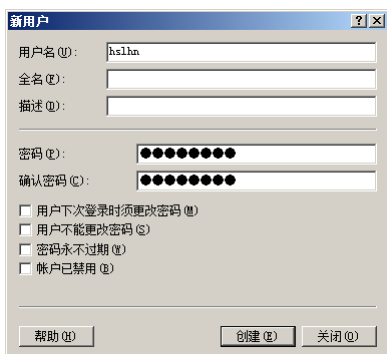


图 13-1 创建用户和组

(1) 应用程序在服务器上运行，一旦服务器出现故障或者重新启动，将直接影响用户的使用。

(2) 默认情况下，用户的数据保存在服务器上。如果服务器出现故障，对用户的数据可能造成影响。

(3) 操作系统兼容性问题：用户使用的应用程序可能受到操作系统版本的限制，在 Windows Server 2008 中存在兼容性的问题。

(4) 数据链路问题：如果用户使用的网络出现问题，桌面虚拟化发布的应用程序不能运行，将直接影响应用程序的使用。

13.1.3 安装终端服务

终端服务默认并没有随系统而安装，需要通过“添加角色向导”来手动安装，操作步骤如下。

① 在安装终端服务之前应根据实际需要创建用户和组，准备赋予终端服务访问权限，如图 13-1 所示。

② 运行“添加角色向导”，在如图 13-2 所示的“选择服务器角色”对话框中选中“终端服务”复选框。

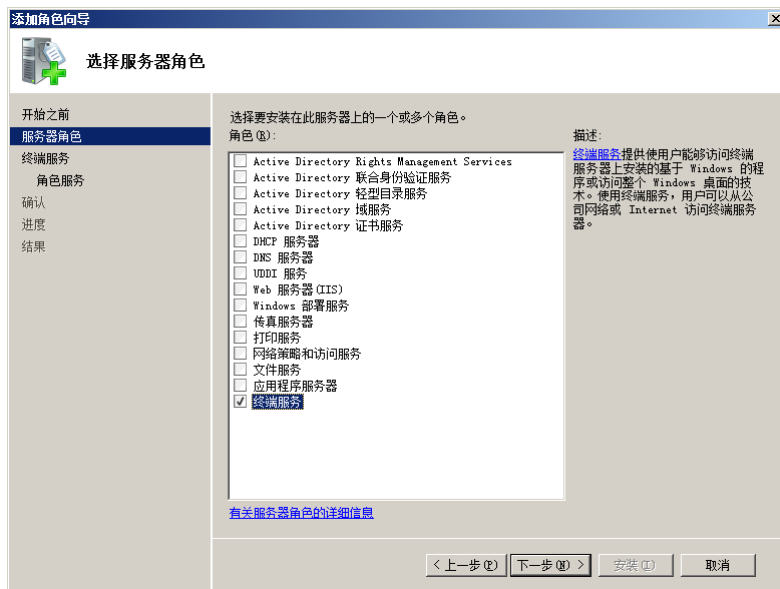


图 13-2 “选择服务器角色”对话框

③ 单击“下一步”按钮，显示如图 13-3 所示“终端服务”对话框。其中显示终端服务的简介及其注意事项，单击“终端服务概述”超级链接可以查看其概述信息。

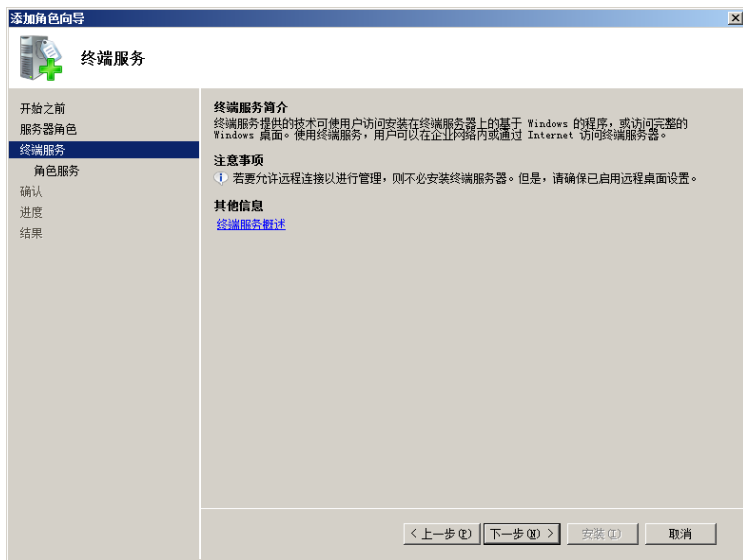


图 13-3 “终端服务”对话框

④ 单击“下一步”按钮，显示如图 13-4 所示的“选择角色服务”对话框。根据需要选中所要安装的组件，这里选择“终端服务器”复选框。

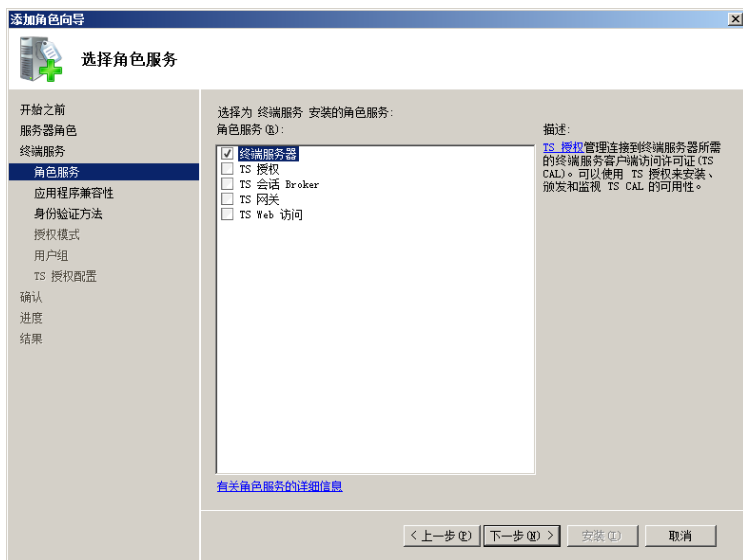


图 13-4 “选择角色服务”对话框

其中的主要选项如下。

终端服务器：安装终端服务器，用户可以连接到终端服务器来运行程序、保存文件，并且使用该服务器上的网络资源。

TS 授权：管理连接到终端服务器所需的终端服务客户端访问许可证（TS CAL），可以使用 TS 授权来安装、颁发和监视该许可证的可用性。

TS 会话 Broker：支持场中终端服务器间的会话负载平衡，并支持与终端服务器（负载平衡终端服务器场的成员）上的现有会话之间的重新连接。

TS 网关：使授权用户能够通过 Internet 连接到企业网络上的终端服务器和远程桌面。

TS Web 访问：提供通过 Web 浏览器访问终端服务器功能。

⑤ 单击“下一步”按钮，显示如图 13-5 所示的“卸载并重新安装兼容的应用程序”对话框。提示用户最好在安装终端服务器后，将希望用户使用的应用程序安装到终端服务器中。需要注意的是，

如果在安装终端服务器之前安装了应用程序，在用户使用时可能会无法正常运行。

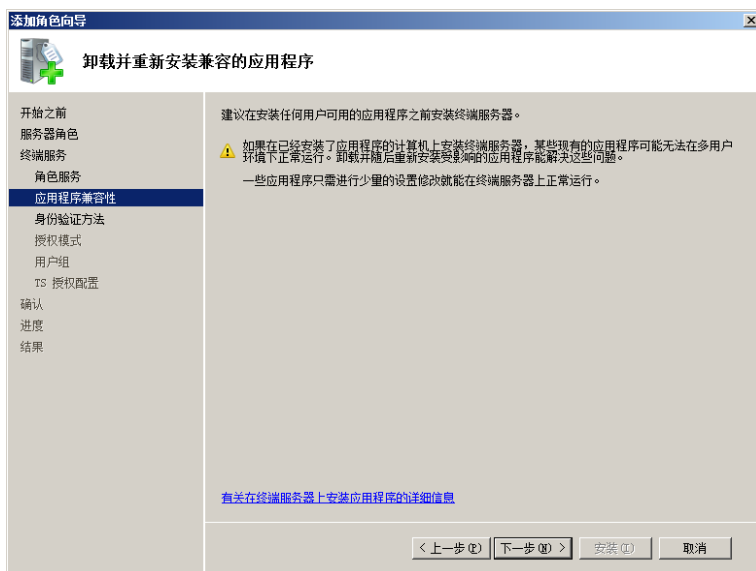


图 13-5 “卸载并重新安装兼容的应用程序”对话框

⑥ 单击“下一步”按钮，显示如图 13-6 所示的“指定终端服务器的身份验证方法”对话框。根据需选择终端服务器的身份验证方法，出于安全考虑建议用户选择要求使用网络级身份验证。

要求使用网络级身份验证：要有计算机同时运行 Windows 版本和支持网络级身份验证的远程桌面连接的客户端版本，才能连接到该终端服务器。

不需要网络级身份验证：任何版本的远程桌面连接客户端都可以连接到该终端服务器。

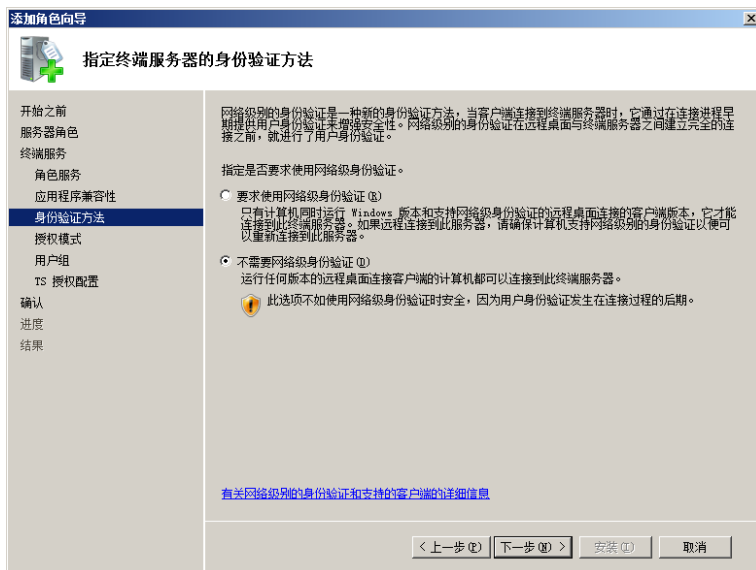


图 13-6 “指定终端服务器的身份验证方法”对话框

提示 网络级别的身份验证是一种新的身份验证方法，当客户端连接到终端服务器时，它通过在连接进程早期提供用户身份验证来增强安全性。在建立完全远程桌面与终端服务器之间的连接之前，使用网络级别的身份验证进行用户身份验证。

⑦ 单击“下一步”按钮，显示如图 13-7 所示的“指定授权模式”对话框。根据实际需要选择终端服务器客户端访问许可证的类型，这里选择“每用户”选项。如果选择“以后配置”单选按钮，则

在接下来的 120 天以内必须配置授权模式。

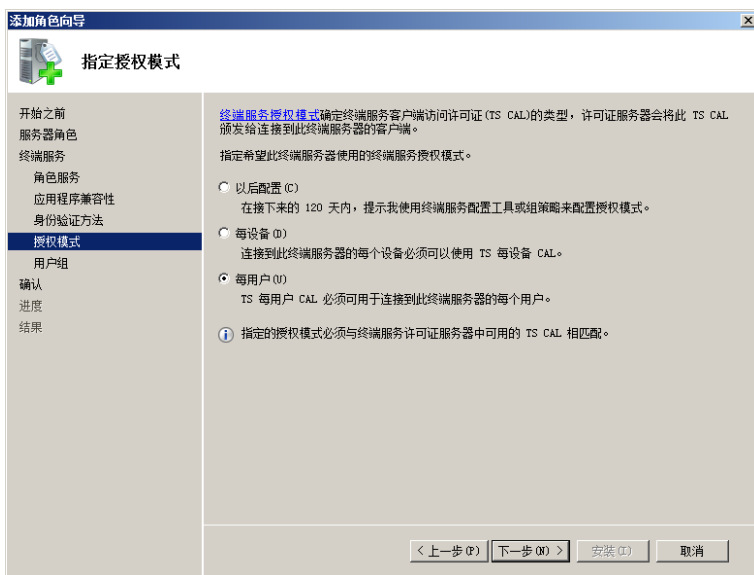


图 13-7 “指定授权模式”对话框

⑧ 单击“下一步”按钮，显示如图 13-8 所示的“选择允许访问终端服务器的用户组”对话框。选择可以连接到该终端服务器的用户组，添加的用户将被添加到“Remote Desktop Users”用户组中。

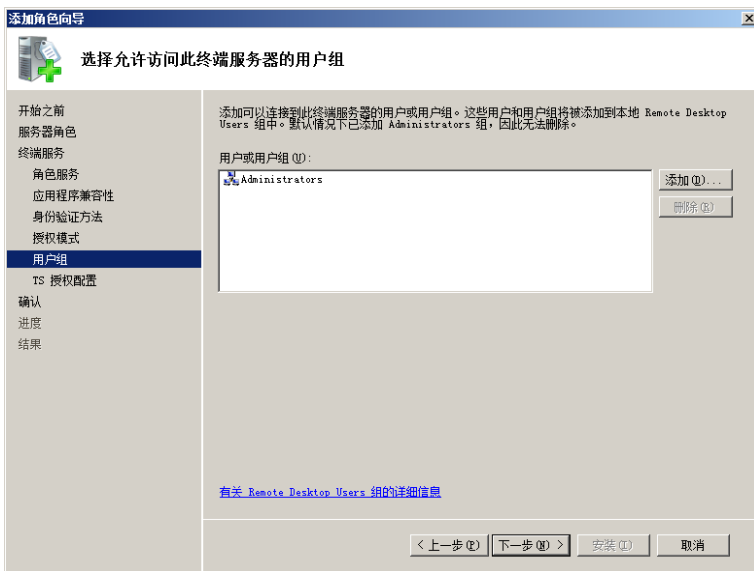


图 13-8 “选择允许访问终端服务器的用户组”对话框

⑨ 单击“添加”按钮，显示如图 13-9 所示的“选择用户”对话框。选择允许使用终端服务的用户，单击“确定”按钮添加。

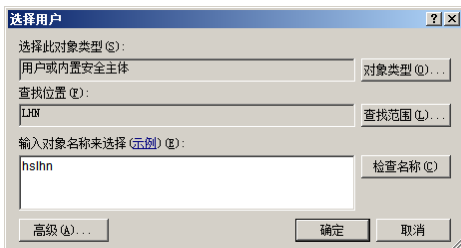


图 13-9 “选择用户”对话框

⑩ 单击“下一步”按钮，显示如图 13-10 所示的“确认安装选择”对话框，其中列出前面所做的配置。



图 13-10 “确认安装选择”对话框

⑪ 单击“安装”按钮开始安装，完成后显示如图 13-11 所示的“安装结果”对话框。



图 13-11 “安装结果”对话框

⑫ 单击“关闭”按钮，显示如图 13-12 所示的“是否希望立即重新启动”对话框。提示必须重新启动计算机，才能完成安装过程；否则无法添加或删除其他角色、角色服务或功能。

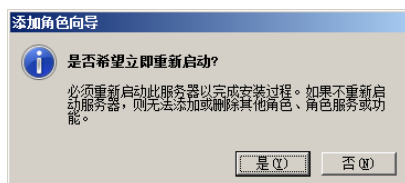


图 13-12 “是否希望立即重新启动”对话框

⑬ 单击“是”按钮，立即重新启动计算机。重启后显示如图 13-13 所示的“安装结果”对话框。单击“关闭”按钮，完成 Windows Server 2008 终端服务的安装。



图 13-13 “安装结果”对话框

单击“开始”→“管理工具”→“终端服务”→“终端服务管理器”选项，显示如图 13-14 所示的“终端服务管理器”窗口，网络管理员可在其中查看当前服务器连接用户、会话，以及进程

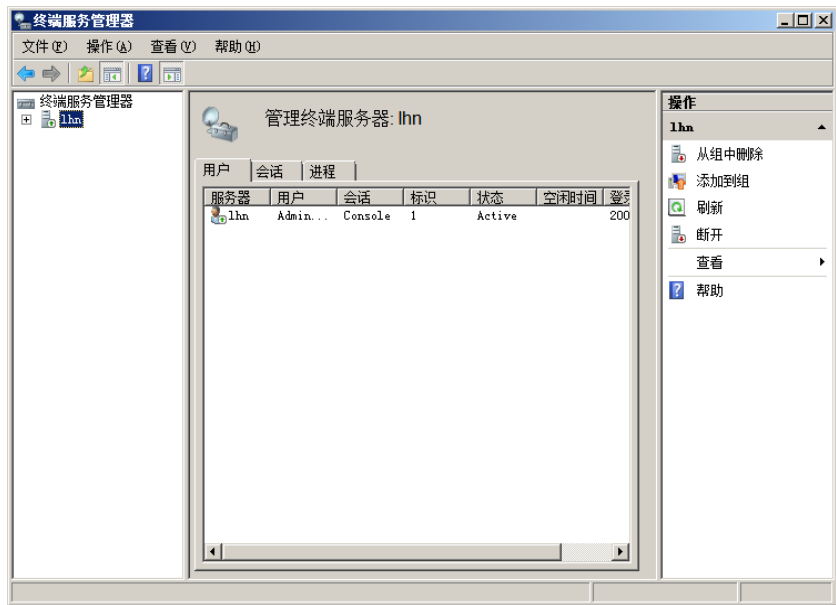


图 13-14 “终端服务管理器”窗口

13.1.4 终端服务器授权

终端服务器安装完成后，需要向终端服务许可证服务器申请许可证，并提示需要配置终端服务许可服务器；否则将会在 120 天之后停止运行终端服务器，如图 13-15 所示。网络管理员需要激活授权服务器，使“终端服务”客户端第 1 次尝试登录终端服务器时，终端服务器会与许可证服务器联系并为该客户端请求许可证。需要注意的是激活服务器时，必须保证已接入 Internet。

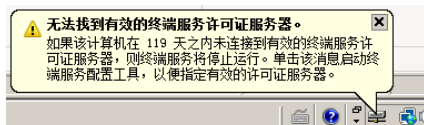


图 13-15 无法找到有效的终端服务许可证服务器

激活授权服务器的步骤如下。

- ① 单击“开始”→“管理工具”→“终端服务器”→“TS 授权管理器”选项，显示如图 13-16 所示的“TS 授权管理器”窗口。默认情况下，TS 授权管理器没有被激活。
- ② 选择服务器名称，右击并选择快捷菜单中的“激活服务器”选项。打开“服务器激活向导”对话框，如图 13-17 所示。

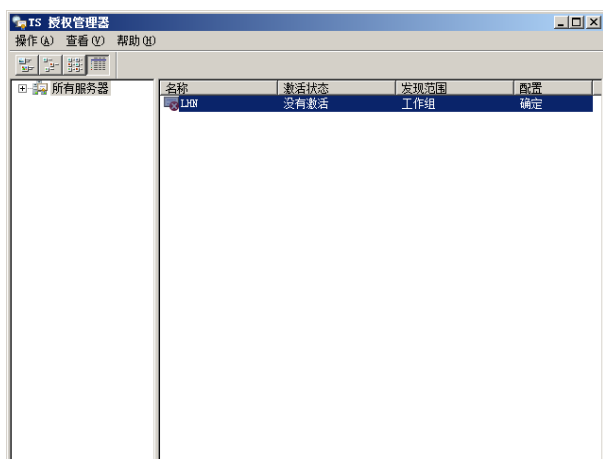


图 13-16 “TS 授权管理器”窗口

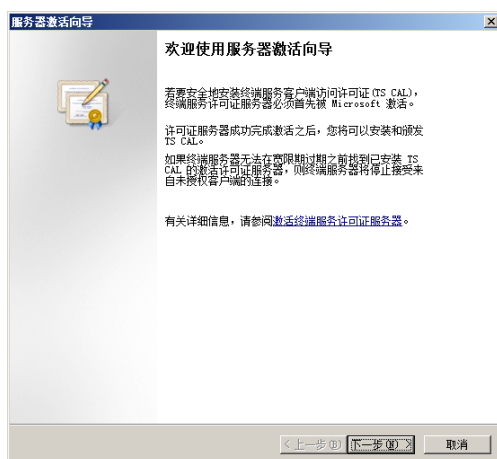


图 13-17 “服务器激活向导”对话框

- ③ 单击“下一步”按钮，显示如图 13-18 所示的“连接方法”对话框，在“连接方法”下拉列表框中选择“自动连接（推荐）”选项即可。
- ④ 单击“下一步”按钮，开始查找激活服务器，并显示如图 13-19 所示的“公司信息”对话框。在“国家（地区）”下拉列表框中选择“中国”选项，并键入公司和姓名信息即可。

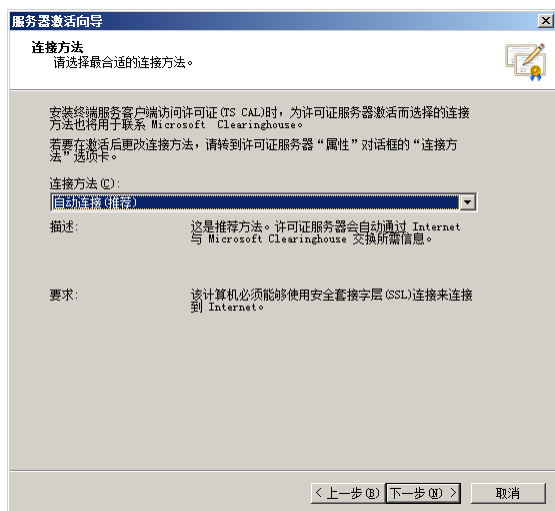


图 13-18 “连接方法”对话框

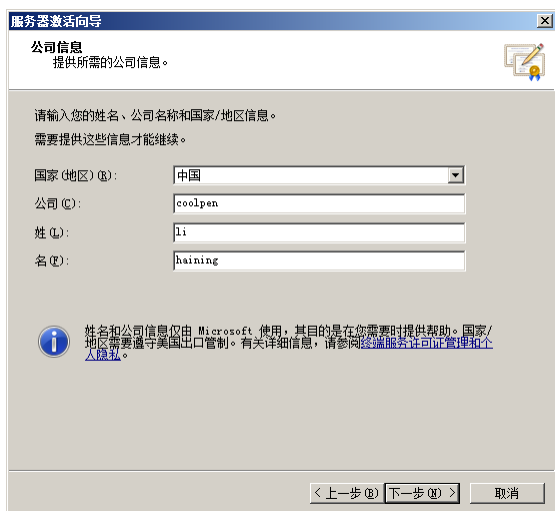


图 13-19 “公司信息”对话框

- ⑤ 单击“下一步”按钮，显示如图 13-20 所示的“公司信息”对话框，键入详细的公司信息。
- ⑥ 单击“下一步”按钮，开始激活许可证服务器。完成后显示如图 13-21 所示的“正在完成服

务器激活向导”对话框，清除“立即启动许可证安装向导”复选框。



图 13-20 “公司信息”对话框

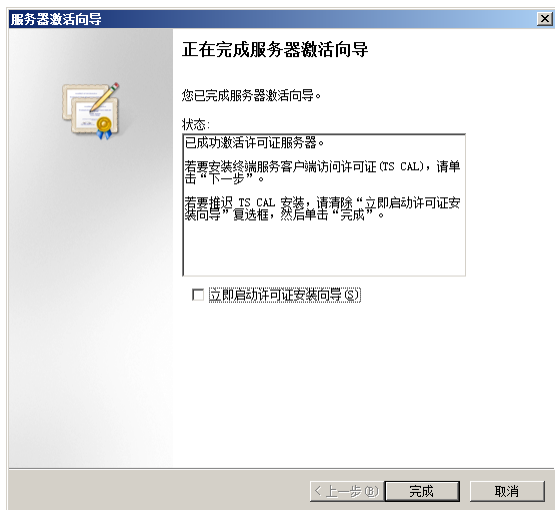


图 13-21 “正在完成服务器激活向导”对话框

⑦ 单击“完成”按钮，返回“TS 授权管理器”窗口。可以看到服务器已被激活，如图 13-22 所示。

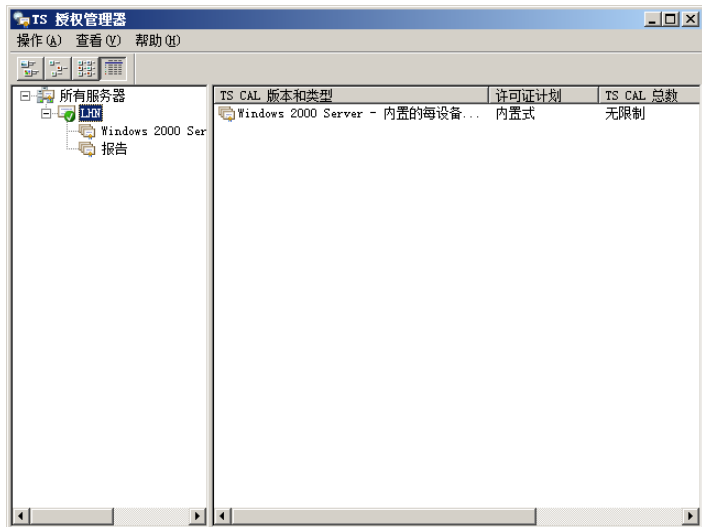


图 13-22 服务器已被激活

13.2 远程桌面连接

对服务器的远程管理通常利用“远程桌面连接”来完成，可使具有相应权限的用户远程登录到服务器的桌面。利用鼠标和键盘操作服务器，运行服务器中的程序并更改系统配置等。如同操作自己的系统一样方便，并且所有的操作都只会在服务器端生效。

13.2.1 在 Windows 9x/2000 客户端上远程管理

Windows 9x/2000 和 Windows XP Home Edition 系统都没有内置远程桌面功能，需要安装 Windows XP Professional 或 Windows Server 2003 终端服务客户端程序。才能用来远程管理服务器。这里以在 Windows 2000 系统中安装 Windows Server 2003 为例介绍。

① 登录到 Windows 2000 系统，将 Windows Server 2003 安装光盘插入 CD-ROM 驱动器，显示如

图 13-23 所示的欢迎页面。



图 13-23 欢迎页面

- ② 单击“执行其他任务”超级链接项图标，显示如图 13-24 所示的“您希望做什么”页面。



图 13-24 “您希望做什么”页面

- ③ 单击“设置远程桌面连接”超级链接项，打开“远程桌面连接-InstallShield 向导”对话框，如图 13-25 所示。

- ④ 单击“下一步”按钮，显示如图 13-26 所示的“许可协议”对话框，选择“我接受许可协议中的条款”单选按钮。



图 13-25 “远程桌面连接安装向导”对话框



图 13-26 “许可协议”对话框

⑤ 单击“下一步”按钮，显示如图 13-27 所示的“客户信息”对话框，在“用户名”和“单位”文本框中分别输入用户名和单位名称。

⑥ 单击“下一步”按钮，显示如图 13-28 所示的“可以安装程序了”对话框，提示用户要开始安装。



图 13-27 “客户信息”对话框



图 13-28 “可以安装程序了”对话框

⑦ 单击“安装”按钮，开始安装远程桌面连接。完成后显示如图 13-29 所示“完成了 InstallShield 向导”对话框，单击“完成”按钮即可。

⑧ 单击“开始”→“程序”→“远程桌面连接”选项，显示如图 13-30 所示的“远程桌面连接”对话框，此时可远程连接到终端服务器桌面。



图 13-29 完成安装

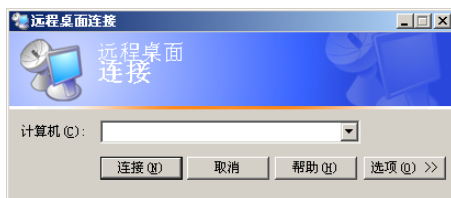


图 13-30 “远程桌面连接”对话框

13.2.2 在 Windows XP/2003/Vista/2008 客户端上远程管理

Windows XP Professional 和 Windows 2003/Vista/2008 都内置有远程桌面功能，可以直接用来远程连接终端服务器的桌面并管理，这里以 Windows Vista 为例。

① 单击“开始”→“所有程序”→“附件”→“远程桌面连接”选项，显示如图 13-31 所示“远程桌面连接”对话框，在“计算机”文本框中输入终端服务器的 IP 地址。

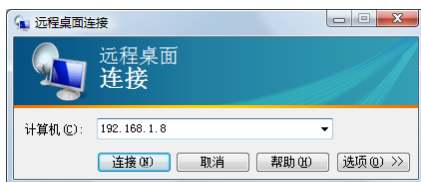


图 13-31 “远程桌面连接”对话框

- ② 单击“选项”按钮，显示如图 13-32 所示的对话框，在其中可以设置远程桌面连接选项。
- ③ 打开“显示”选项卡，如图 13-33 所示。在其中可以设置远程桌面的大小及颜色质量，通常应根据显示器的分辨率大小来设置。

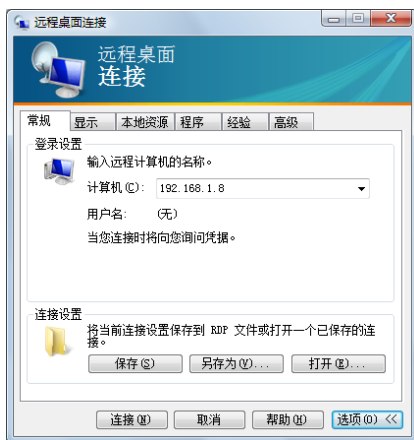


图 13-32 设置远程桌面连接选项

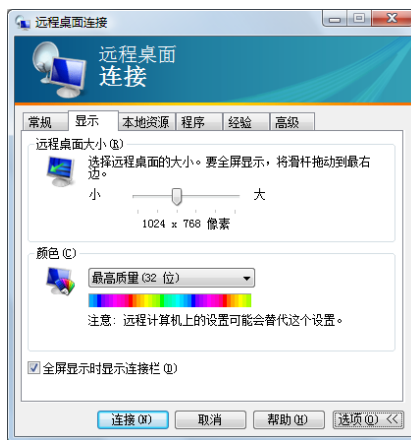


图 13-33 “显示”选项卡

- ④ 打开“本地资源”选项卡，如图 13-34 所示，在其中可以设置要使用的本地资源。
- ⑤ 打开“程序”选项卡，如图 13-35 所示，在其中可以配置在使用远程桌面连接时启动的程序。



图 13-34 “本地资源”选项卡



图 13-35 “程序”选项卡

- ⑥ 打开“经验”选项卡，如图 13-36 所示。在其中根据网络状况选择连接速度，以优化性能。
- ⑦ 打开“高级”选项卡，如图 13-37 所示，在其中可以设置服务器身份验证的使用方式。

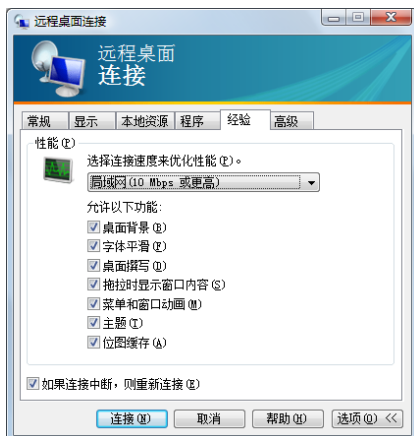


图 13-36 “经验”选项卡

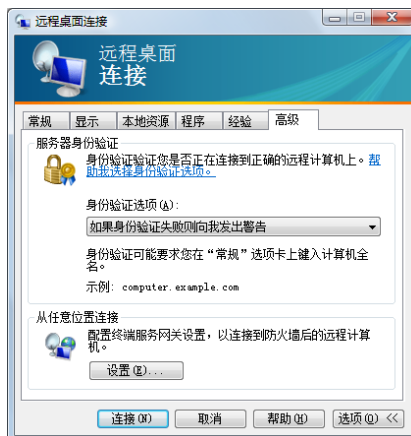


图 13-37 “高级”选项卡

⑧ 设置完成后单击“连接”按钮，显示如图 13-38 所示的“Windows 安全”对话框，分别在“用户名”和“密码”文本框中输入访问服务器的用户名和密码。

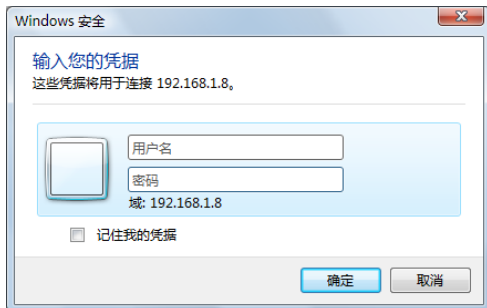


图 13-38 “Windows 安全”对话框

⑨ 单击“确定”按钮，远程连接到服务器的桌面，如图 13-39 所示。此时用户可以像使用本地计算机一样，根据所具有的权限利用键盘和鼠标操作服务器。



图 13-39 远程服务器桌面

13.3 使用 Web 方式远程管理

如果客户端上没有远程桌面组件，也可以使用 Web 方式，利用 IE 浏览器来远程管理服务器。当然，终端服务器必须安装相应的 Web 访问组件。而客户端只要安装有 IE 浏览器，即可通过局域网或 Internet 实现远程管理，并且操作服务器的方式和远程桌面一样。

13.3.1 安装远程桌面 Web 连接组件

安装远程桌面 Web 连接组件的操作步骤如下。

① 打开“服务器管理器”控制台，在左侧控制台树中选择“角色”选项。然后在右窗格中单击“终端服务”选项组中的“添加角色服务”超级链接，显示如图 13-40 所示的“选择角色服务”对话框。

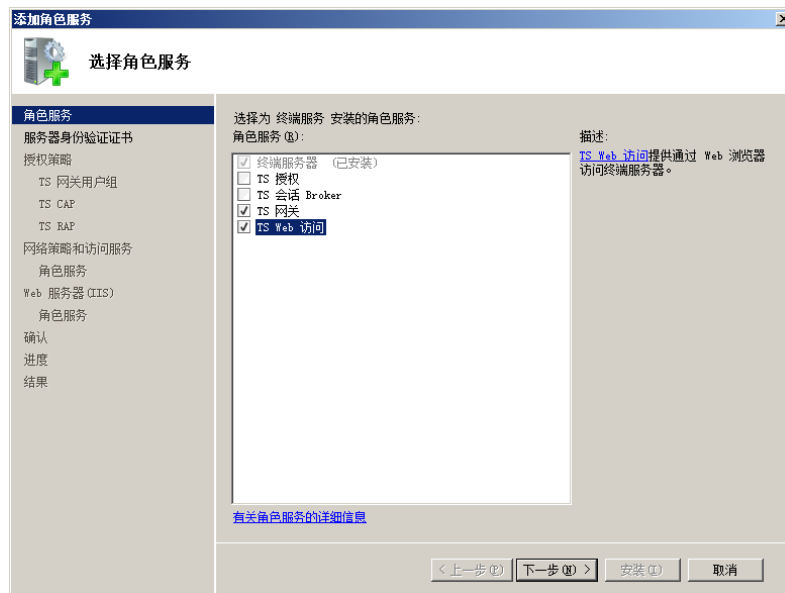


图 13-40 “选择角色服务”对话框

② 选中“TS 网关”和“TS Web 访问”复选框，将会分别显示如图 13-41 所示的“添加角色服务”对话框，提示需要添加相应服务所需要角色和功能。



图 13-41 “添加角色服务”对话框

③ 单击“下一步”按钮，显示如图 13-42 所示的“选择 SSL 加密的服务器身份验证证书”对话框。客户端和服务端通信时需要使用 SSL 加密模式以保护数据的传输安全，因此需要使用数字证书。其中，“为 SSL 加密选择现有证书”模式适合于 Active Directory 环境中，在企业内部创建 CA 根目录服务器时使用；“为 SSL 加密创建自签名证书”模式则适合于在规模较小或者测试的网络中使用。

④ 单击“下一步”按钮，显示如图 13-43 所示的“为 TS 网关创建授权策略”对话框。连接授权策略 (TS CAP) 用来指定可以连接到此 TS 网关的用户，如果要现在创建授权策略，则选择“现在”单选按钮；如果要在终端服务管理控制台中设置，则选择“以后”单选按钮。

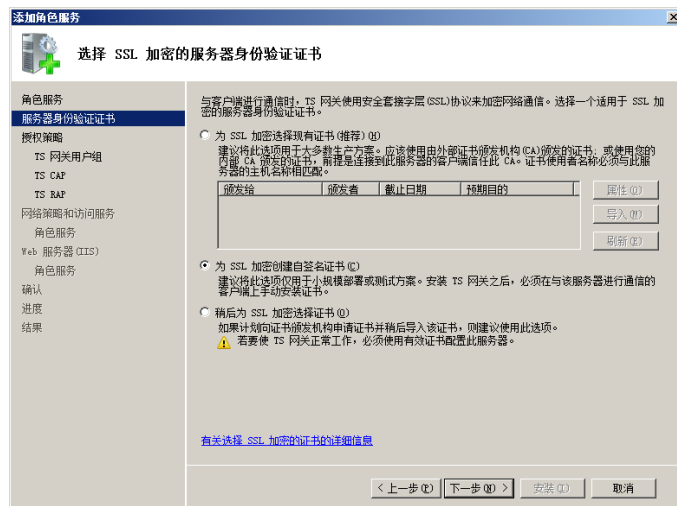


图 13-42 “选择 SSL 加密的服务器身份验证证书”对话框



图 13-43 “为 TS 网关创建授权策略”对话框

⑤ 单击“下一步”按钮，显示如图 13-44 所示的“选择可以通过 TS 网关连接的用户组”对话框，在其中添加可通过 TS 网关的用户组。

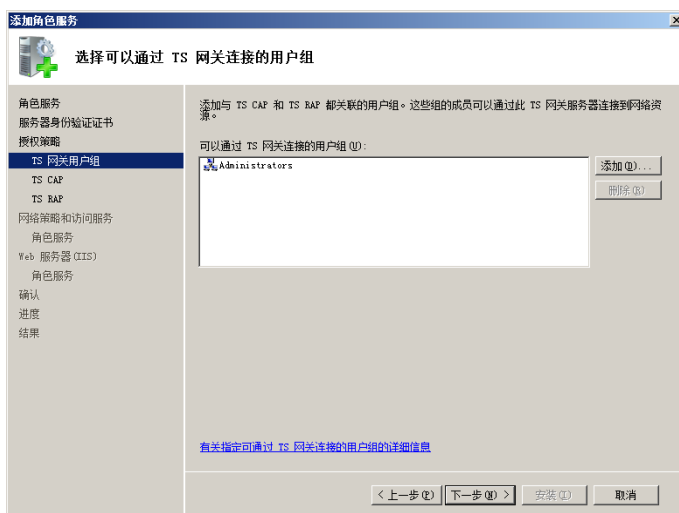


图 13-44 “选择可以通过 TS 网关连接的用户组”对话框

⑥ 单击“添加”按钮，显示如图 13-45 所示的“选择组”对话框。在“输入对象名称来选择”文本框中输入待授权的用户组名称，单击“确定”按钮添加。

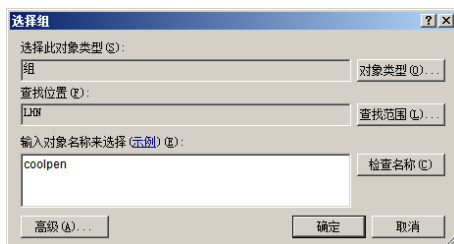


图 13-45 “选择组”对话框

⑦ 单击“下一步”按钮，显示如图 13-46 所示的“为 TS 网关创建 TS CAP”对话框。需要创建一个连接授权策略，以允许用户连接到此 TS 网关服务器。在“输入 TS CAP 的名称”文本框中为连接授权策略设置一个名称，并选择一种身份验证方式，这里选择“密码”模式。

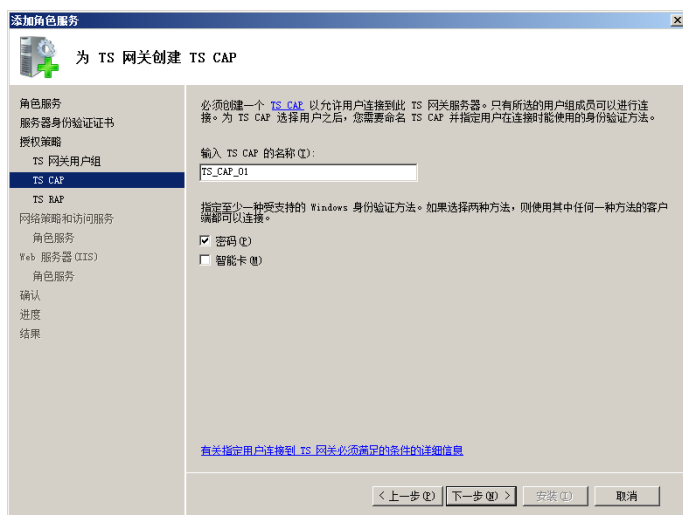


图 13-46 “为 TS 网关创建 TS CAP”对话框

⑧ 单击“下一步”按钮，显示如图 13-47 所示的“为 TS 网关创建 TS RAP”对话框。在“输入 TS RAP 的名称”文本框中输入资源授权策略的名称，并指定可通过此资源授权策略访问的计算机，这里选择“允许用户连接到网络上的任何计算机”单选按钮。

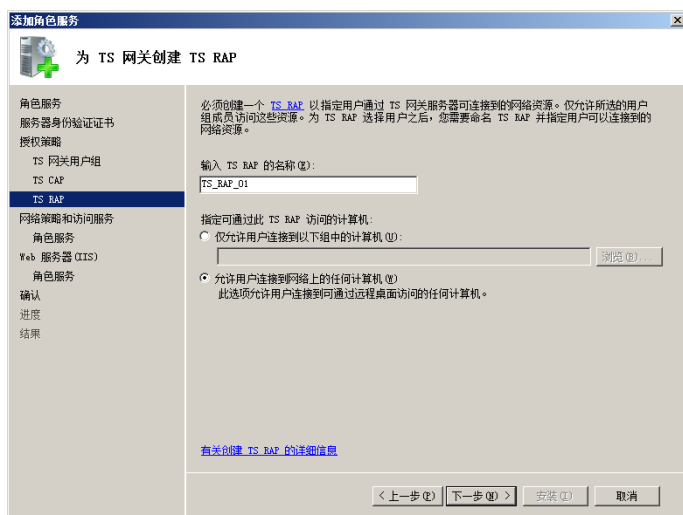


图 13-47 “为 TS 网关创建 TS RAP”对话框

⑨ 单击“下一步”按钮，显示如图 13-48 所示的“网络策略和访问服务”对话框，其中显示网络策略和访问服务的概述信息和注意事项。



图 13-48 “网络策略和访问服务”对话框

⑩ 单击“下一步”按钮，显示如图 13-49 所示的“选择角色服务”对话框。在“角色服务”列表框中选中“网络策略服务器”复选框，使用网络策略服务器提供安全策略。

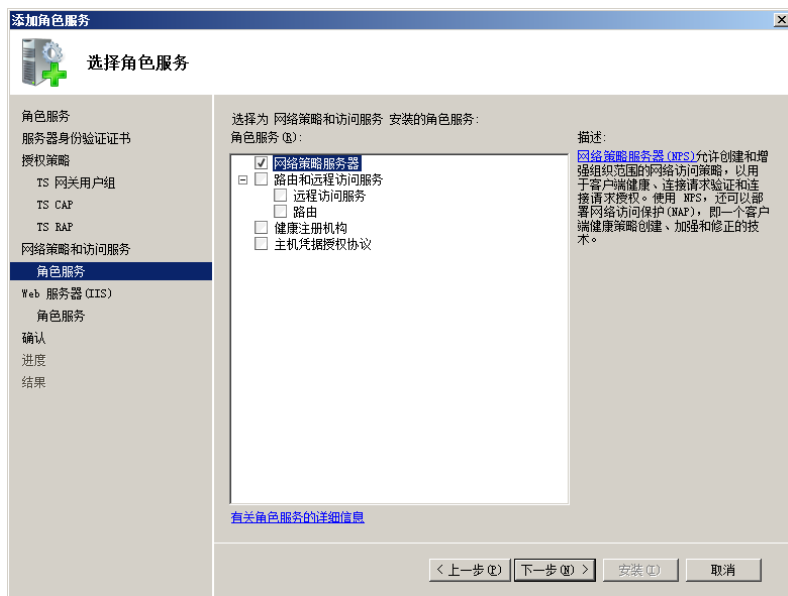


图 13-49 “选择角色服务”对话框

⑪ 单击“下一步”按钮，显示如图 13-50 所示的“Web 服务器 (IIS)”对话框，其中简单介绍了 IIS 服务。

⑫ 单击“下一步”按钮，显示如图 13-51 所示的“选择角色服务”对话框，默认已经选择需要的功能。



图 13-50 “Web 服务器 (IIS)” 对话框



图 13-51 “选择角色服务” 对话框

⑬ 单击“下一步”按钮，显示如图 13-52 所示的“确认安装选择”对话框。其中显示前面所做的配置，如果需要更改，则单击“上一步”按钮返回。



图 13-52 “确认安装选择” 对话框

⑭ 单击“安装”按钮开始安装选择的服务，安装完成后显示如图 13-53 所示的“安装结果”对话框。



图 13-53 “安装结果”对话框

⑮ 单击“关闭”按钮，此时客户端可以以 Web 方式远程管理服务器。

13.3.2 使用 IE 远程管理

使用 IE 远程管理服务器的操作步骤如下。

① 打开 IE 浏览器，在地址栏中输入终端服务器的网址 `http://服务器名或 IP 地址/ts`。按回车键，显示如图 13-54 所示的登录框，在“用户名”和“密码”文本框中输入具有访问终端服务权限的用户名和密码。

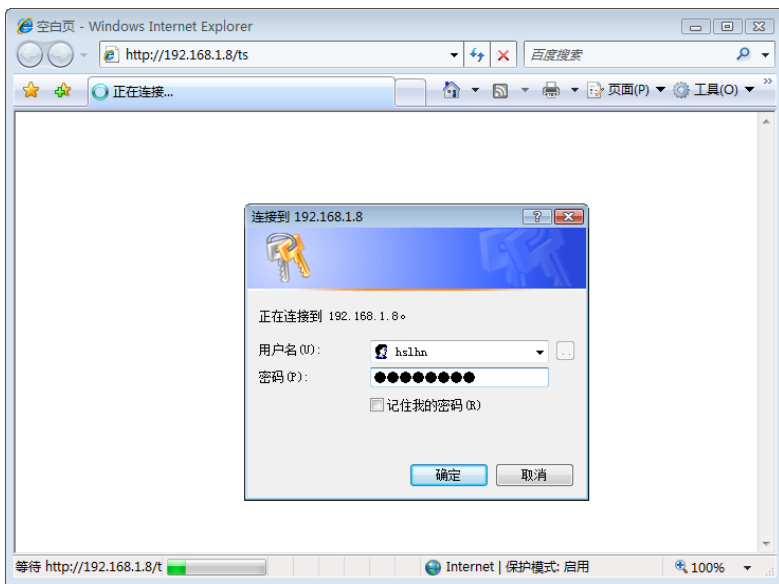


图 13-54 登录框

② 单击“确定”按钮，显示如图 13-55 所示的“TS Web 访问”窗口，其中提示需要安装 ActiveX 控件。



图 13-55 “TS Web 访问”窗口

③ 右击信息栏并选择快捷菜单中的“运行 ActiveX 控件”选项，显示如图 13-56 所示的“安全警告”对话框，询问是否运行该 ActiveX 控件。



图 13-56 “安全警告”对话框

④ 单击“运行”按钮安装此控件，然后单击“远程桌面”按钮，显示如图 13-57 所示的“远程桌面”窗口，提示需要安装“终端服务 ActiveX 客户端”控件。

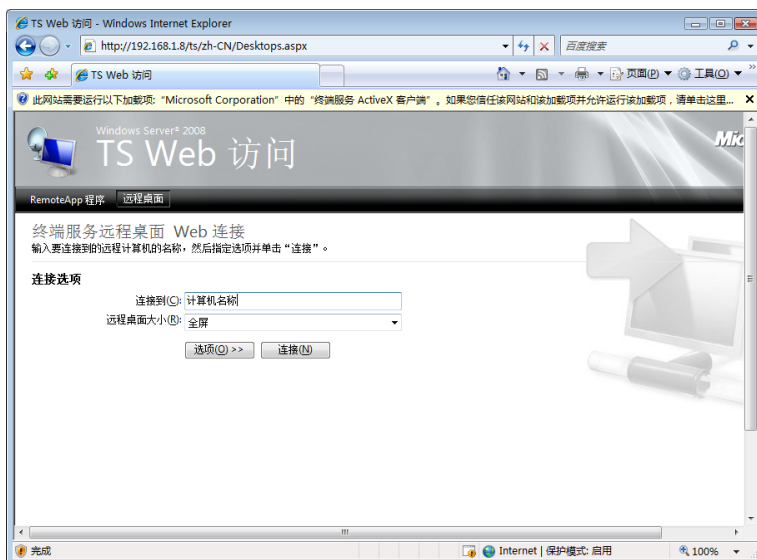


图 13-57 “远程桌面”窗口

⑤ 右击信息栏并选择快捷菜单中的“运行此 ActiveX 控件”选项，显示如图 13-58 所示的“安全警告”对话框，提示是否运行该 ActiveX 控件。



图 13-58 “安全警告”对话框

⑥ 单击“运行”按钮，运行该 ActiveX 控件。然后在“连接到”文本框中输入终端服务器的 IP 地址，在“远程桌面大小”下拉列表框中选择要使用的桌面大小。单击“选项”按钮，还可以设置更详细的选项，如图 13-59 所示。



图 13-59 设置更详细的选项

⑦ 单击“连接”按钮，显示如图 13-60 所示的“远程桌面连接”对话框，其中提示是否使用所选资源。

⑧ 单击“连接”按钮，显示如图 13-61 所示的“输入您的凭据”对话框，在“用户名”和“密码”文本框中分别输入具有登录终端服务器权限的用户账户和密码。

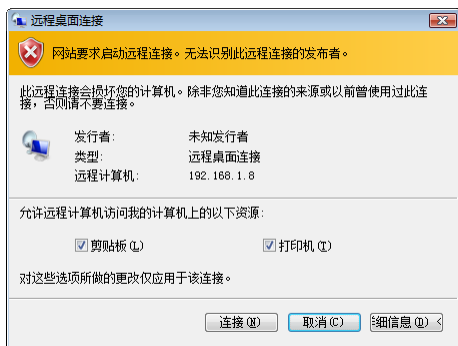


图 13-60 “远程桌面连接”对话框

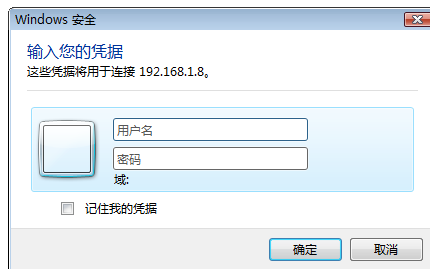


图 13-61 “输入您的凭据”对话框

⑨ 单击“确定”按钮，开始连接远程服务器并自动登录。显示 Windows Server 2008 桌面，如图 13-62 所示。

此时，即可如同使用 Windows 远程桌面一样，在 Windows Server 2008 中执行各种操作。

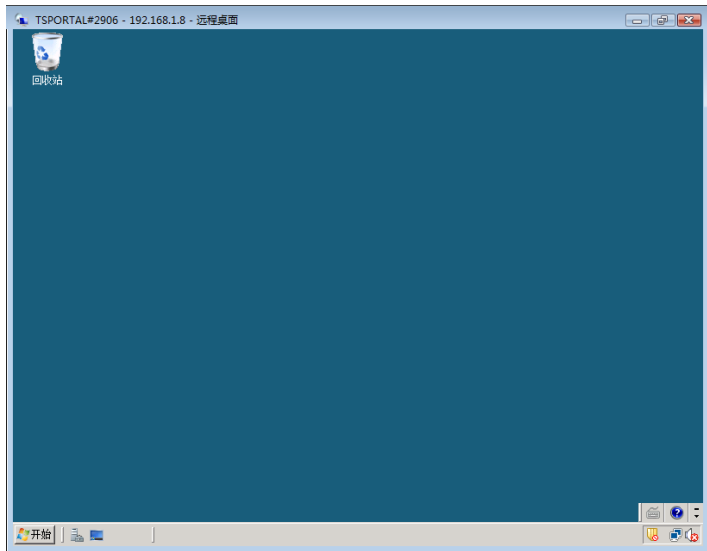


图 13-62 Windows Server 2008 桌面

13.4 应用程序虚拟化

Windows Server 2008 提供了应用程序虚拟化功能，这是 Windows 2000/2003 中没有的功能。利用虚拟化，授权用户可以在客户端运行安装在终端服务器上的应用程序。客户端上仅显示更新内容，并可通过键盘和鼠标与终端服务器的交互信息。利用这个功能，多个用户可以同时使用终端服务器上的程序，而不必在客户端上安装。

13.4.1 发布应用程序

发布应用程序可使用“TS RemoteApp 管理器”来完成，但首先需要将应用程序安装到终端服务器。“TS RemoteApp 管理器”提供的“RemoteApp 向导”用来帮助网络管理员完成应用程序的发布。

- ① 在终端服务器上安装待发布的应用程序。
- ② 单击“开始”→“管理工具”→“终端服务”→“TS RemoteApp 管理器”选项，显示如图 13-63 所示的“TS RemoteApp 管理器”窗口。

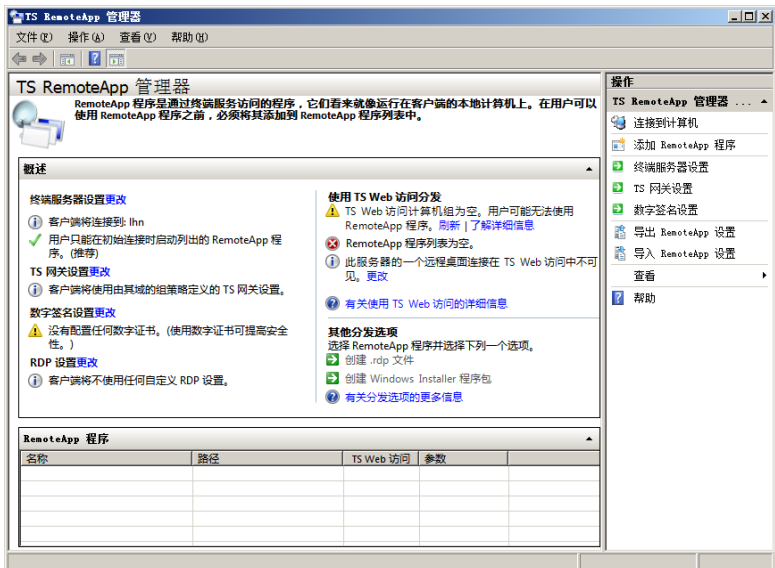


图 13-63 “TS RemoteApp 管理器”窗口

③ 右击“RemoteApp 程序”选项区域中的“名称”列表框，选择快捷菜单中的“添加 RemoteApp 程序”选项。打开“RemoteApp 向导”对话框，如图 13-64 所示。

④ 单击“下一步”按钮，显示如图 13-65 所示的“选择要添加到 RemoteApp 程序列表的路径”对话框。在“名称”列表框中选中要发布的程序复选框，例如“Adobe Photoshop CS3”。

⑤ 单击“下一步”按钮，显示如图 13-66 所示的“复查设置”对话框，其中显示所选设置。

⑥ 单击“完成”按钮，一个应用程序发布完成，如图 13-67 所示。按照同样操作，可发布多个应用程序。

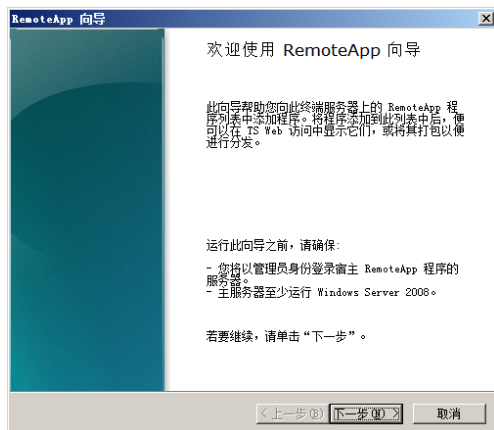


图 13-64 “RemoteApp 向导”对话框



图 13-65 “选择要添加到 RemoteApp 程序列表的路径”对话框

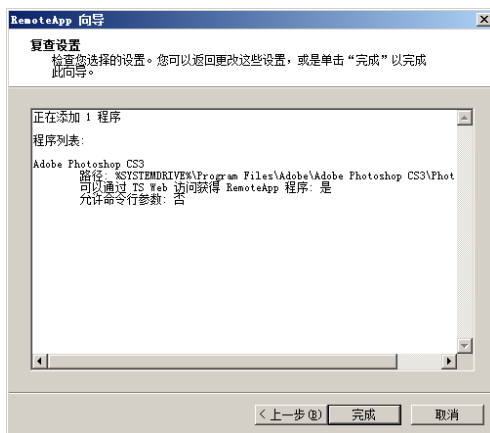


图 13-66 “复查设置”对话框

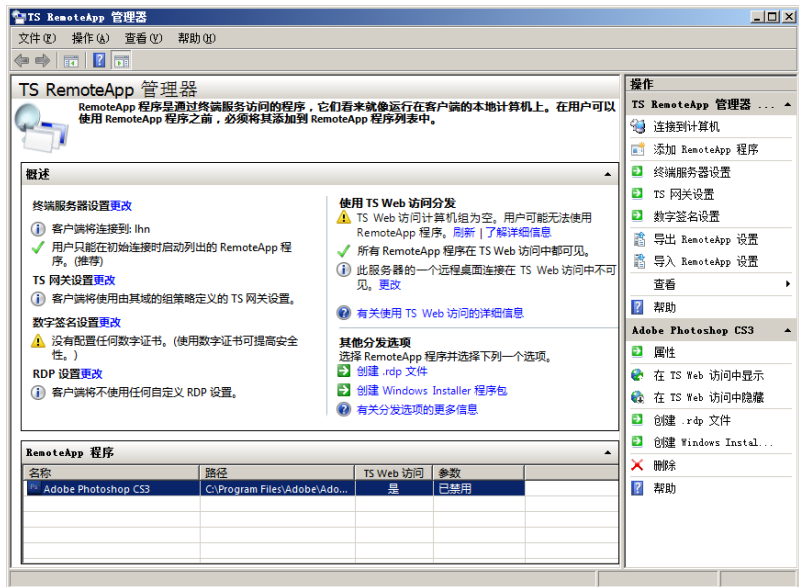


图 13-67 一个应用程序发布完成

13.4.2 创建 RDP 文件

RDP 文件是 Windows Server 2008 桌面虚拟化应用的远程链接文件，“TS RemoteApp 管理器”提供了创建该文件的功能，可将发布的应用程序信息封装成 RDP 文件。用户在安装了 RDP 6.0 的客户端

上执行这个文件，即可实现对应用程序的远程访问，而应用程序其实只在终端服务器中运行。

① 在“TS RemoteApp 管理器”窗口的“RemoteApp”选项组中选择需要发布的应用程序，例如“Adobe Photoshop CS3”。然后在“概述”区域的“其他分发选项”选项组单击“创建.RDP 文件”超级链接，打开“RemoteApp 向导”对话框，如图 13-68 所示。

② 单击“下一步”按钮，显示如图 13-69 所示的“指定程序包位置”对话框。在其中可以设置 RDP 文件的保存位置、TS 网关的参数和证书等，也可使用默认设置。

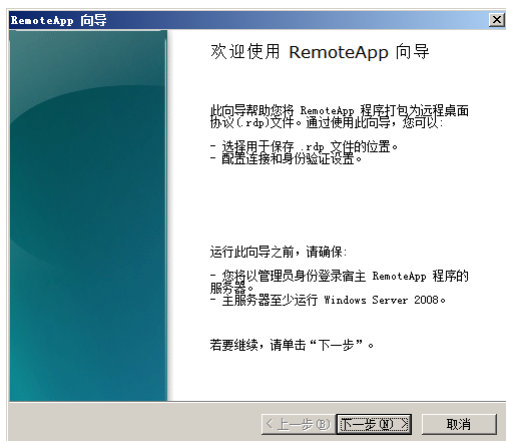


图 13-68 “RemoteApp 向导”对话框

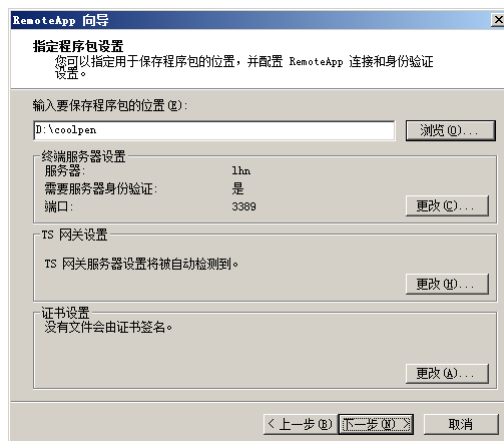


图 13-69 “指定程序包位置”对话框

③ 单击“下一步”按钮，显示如图 13-70 所示的“复查设置”对话框，在其中显示即将创建的 RDP 文件设置。

④ 单击“完成”按钮，创建完成 RDP 文件，如图 13-71 所示。

RDP 文件很小，只有 2 KB。网络管理员可以将其通过 E-mail、组策略或者共享等各种方式发布到客户端中，用户使用该文件即可访问该应用程序。



图 13-70 “复查设置”对话框

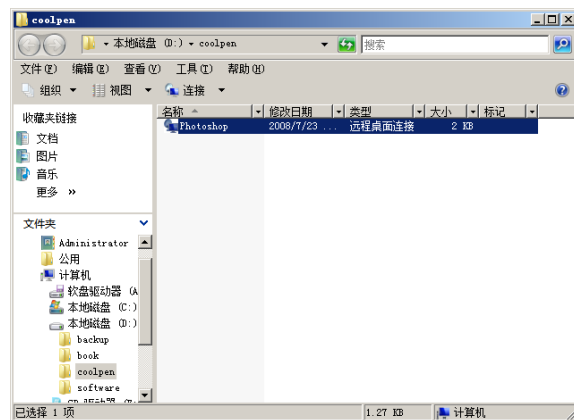


图 13-71 RDP 文件

13.4.3 访问应用程序

当在 Windows Server 2008 终端服务器上发布了应用程序以后，在客户端就可以访问并运行所发布的应用程序。用户可以使用键盘和鼠标操作应用程序，此时应用程序实际上只是在终端服务器上运行。所编辑的文件既可以保存在终端服务器，也可以保存在客户端中。

1. 应用程序访问方式

Windows Server 2008 提供了 3 种方式用来访问所发布的虚拟应用程序，分别是远程桌面、Web 方式和 RDP 远程连接文件方式。

(1) 远程桌面方式：用户使用远程桌面程序或者 IE 浏览器连接并使用“远程桌面”功能，连接到终端服务器后即可运行发布的应用程序。不过使用这种方式时只要具有相应的权限，用户也可运行其他程序以及更改系统配置，因此安全性较低。

(2) Web 方式：利用 IE 浏览器连接终端服务器，并在“RemoteApp 程序”中运行已发布的应用程序。

(3) RDP 连接文件：需要网络管理员将 RDP 部署到客户端，用户以应用程序模式访问。

其中使用后两种方式时，用户只能访问已发布的应用程序，而不能运行其他未发布的程序。并且无法对系统进行操作，因此安全性比较高，也是最常用的访问方式。不过使用这两种方式，客户端需要安装 RDP 6.0 版本的客户端程序。

2. Web 方式访问应用程序

Windows XP、Windows Vista 和 Windows Server 2008 系统使用 IE 浏览器访问发布的应用程序的方式相同，这里以 Windows Vista 为例介绍。

(1) 在客户端打开 IE 浏览器，在地址栏中输入 `http://终端服务器 IP 地址/TS`。并使用具有访问权限的用户账户登录，显示如图 13-72 所示的“TS Web 访问”窗口，在“RemoteApp 程序”窗格中显示已经发布的应用程序。

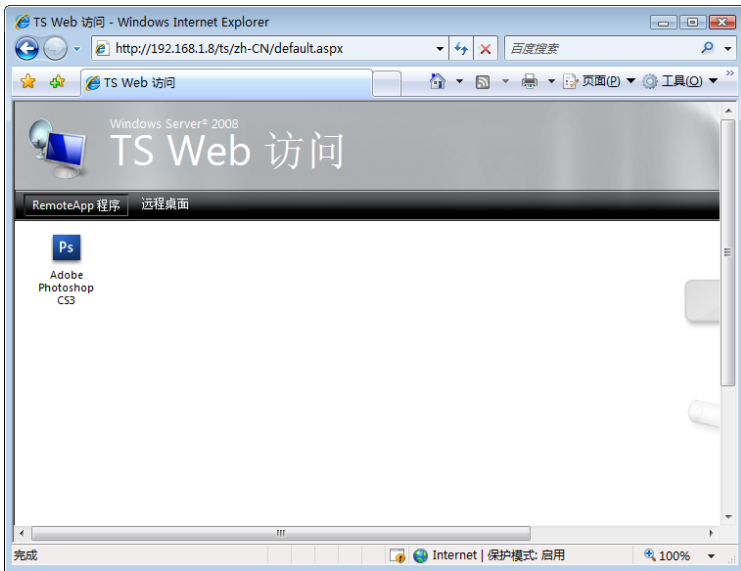


图 13-72 “TS Web 访问”窗口



提示

如果以前没有以 Web 方式访问过终端服务器，则会提示需要安装“终端服务 ActiveX 客户端”控件，只有安装了该控件才能使用。

(2) 单击要访问的应用程序，如“Adobe Photoshop CS3”按钮。显示如图 13-73 所示的“RemoteApp”对话框，根据需要选择终端服务器可以访问本地计算机的资源。

(3) 单击“连接”按钮，显示如图 13-74 所示的“输入您的凭据”对话框，输入具有访问终端服务器权限的用户名及密码。

(4) 单击“确定”按钮，即可连接到终端服务器。连接成功后，运行“Adobe Photoshop CS3”并可使用，如图 13-75 所示。

(5) 如果要打开或者保存文件，可在“查找范围”下拉列表框中选择打开或保存在终端服务器中或者本地计算机中，如图 13-76 所示，默认为终端服务器。

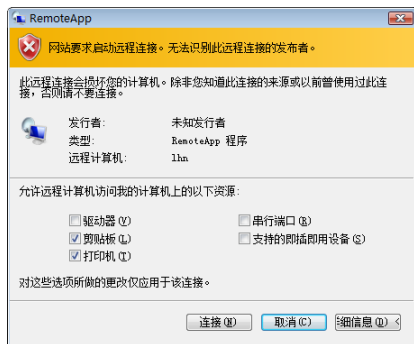


图 13-73 “RemoteApp”对话框

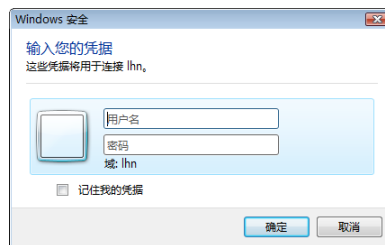


图 13-74 “输入您的凭据”对话框

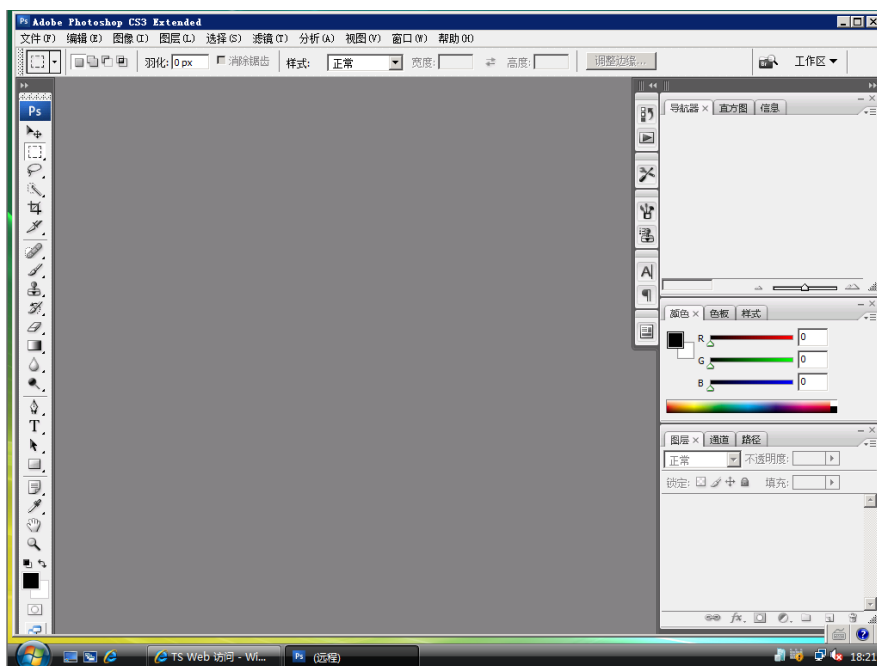


图 13-75 运行应用程序

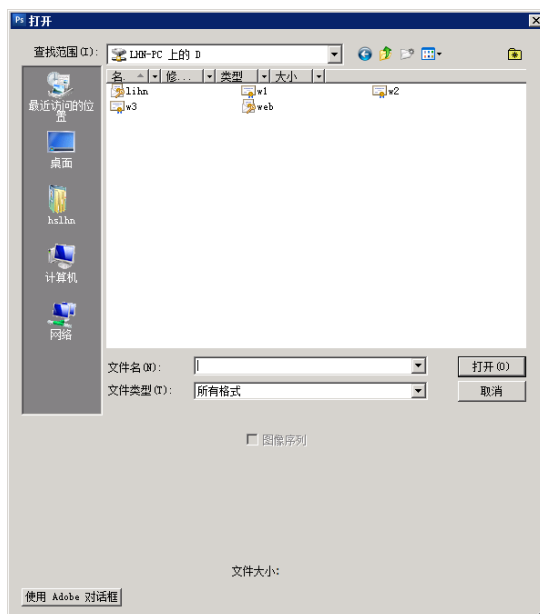


图 13-76 打开文件

3. RDP 连接文件访问应用程序

当终端服务器上创建的 RDP 连接文件并发布到客户端上以后,用户直接运行该文件即可连接到终端程序,并运行所发布的虚拟应用程序。由于 Windows Vista 和 Windows Server 2008 系统均内置了 RDP 6.0 版本的客户端程序,因此使用方法相同,这里以 Windows Vista 为例介绍。

(1) 将已创建的 RDP 文件复制到客户端上后双击运行,显示如图 13-77 所示的“RemoteApp”对话框。

(2) 单击“连接”按钮,显示如图 13-78 所示的“输入您的凭据”对话框,在其中输入具有访问权限的用户名及密码。

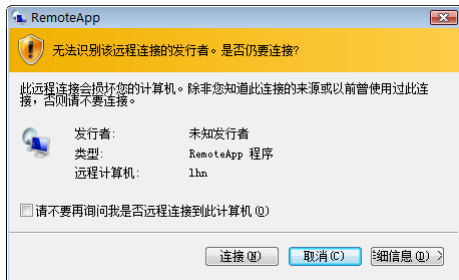


图 13-77 “RemoteApp”对话框

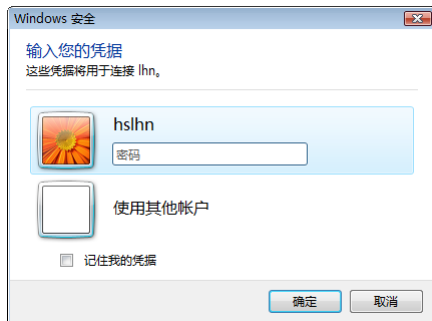


图 13-78 “输入您的凭据”对话框

(3) 单击“确定”按钮,即可运行该应用程序,如图 13-79 所示。

4. Windows XP

要使用 RDP 连接文件来访问虚拟应用程序,系统中必须安装远程连接客户端程序 RDP 6.0 版本。Windows XP SP3 已经内置了 RDP 6.0,但 Windows XP SP2 中的版本仅为 RDP 5.1,必须升级为版本 RDP 6.0 才能访问 Windows Server 2008 发布的虚拟应用程序。升级到 RDP 6.0 以后,访问应用程序的方式和 Windows Vista/2008 相同。需要注意的是,RDP 方式只适用于 Windows XP/2003,不能在 Windows 9x/2000 中运行。

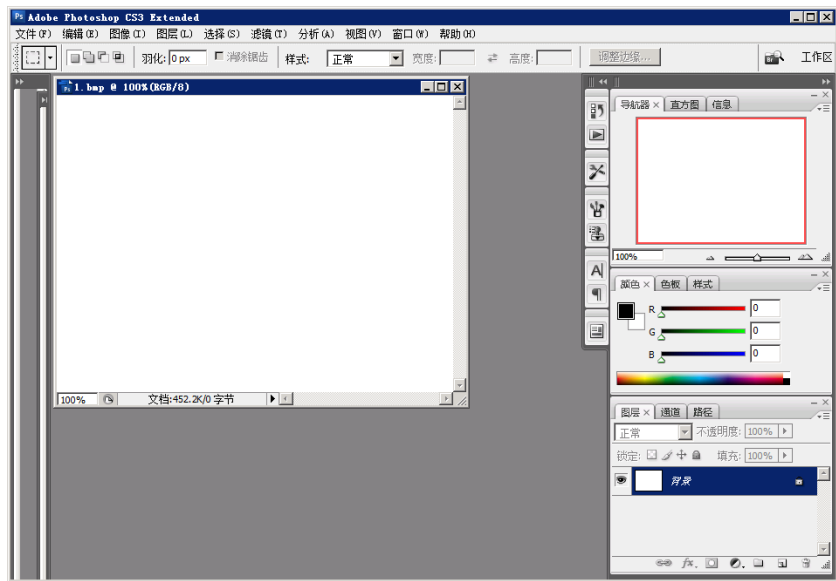


图 13-79 运行应用程序

RDP 6.0 的下载页面地址为 <http://support.microsoft.com/default.aspx/kb/925876>,下载页面如图 13-80 所示,用户应根据所使用的操作系统下载相应版本的 RDP 程序。

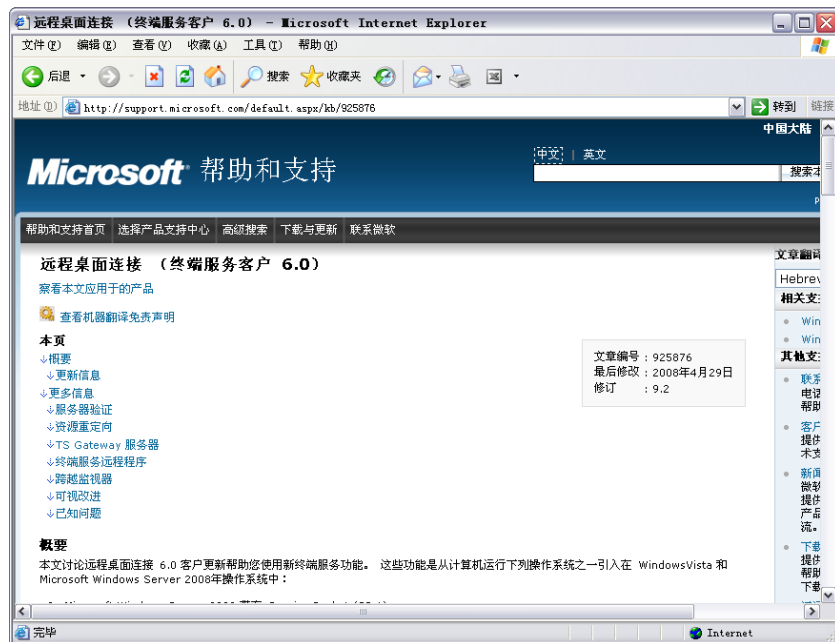


图 13-80 RDP 下载页面

下载 RDP 6.0 到本地后，直接安装即可。安装完成后，即可使用 RDP 连接文件来访问 Windows Server 2008 发布的虚拟应用程序。具体操作请参见前面所述的内容，这里不再赘述。

第 14 章 配置与管理远程安装服务

远程安装服务（Remote Installation Service, RIS）可以为支持 PXE 远程启动的计算机部署新的操作系统，在 Windows Server 2003 系统下主要用来部署 Windows XP Professional 或 Windows 2000 Professional 操作系统，也可以部署 Windows 2000 Server 或 Windows Server 2003。更早版本的 Windows 2000 RIS 服务器只能部署工作站版本，即 Professional 版本，而 Windows Server 2003 的 RIS 可以部署全系列的 Windows 2000 以上的产品。

14.1 远程安装服务与 Windows 部署服务概述

远程安装服务与 Windows 部署服务是具有相同功能的软件，前者出现的时间比较早一些；后者则功能更为强大，操作更加简单。

14.1.1 远程安装服务简介

利用 RIS 可以部署大量 Windows 2000 Professional 或者 Windows XP Professional 系统，客户端只需安装支持 PXE 引导的网卡即可利用这套工具快速地安装 Windows 2000 Professional 或者 Windows XP Professional。目前基本上所有的网卡，无论是集成网卡，还是独立网卡均支持 PXE 引导技术。RIS 服务器配置完成后，在客户端计算机上只需要开机后按 F12 键，即可安装操作系统。

使用 RIS 可以执行以下操作。

(1) 用户启动客户端时，即使该计算机没有操作系统，RIS 服务器通过从网络安装操作系统也能响应，无须光盘。为了支持该功能，客户端计算机必须使用“预启动执行环境”（PXE），这是一种允许客户端计算机从网络适配器开始启动序列的远程启动技术。

(2) 提供包括特定设置和应用程序的操作系统映像（例如，符合某个企业桌面标准的映像），可以为特定组的用户提供分配给该组的一个或多个映像。

(3) 为 Windows Server 2003 家族中的产品创建自动安装映像，并创建 Windows XP 和 Windows 2000 的映像。

一 提 示



在 Windows 2000 Server 的远程安装服务中，只支持 Windows 2000 Professional，不支持 Windows 2000 Server 系列的远程安装。在 Windows Server 2003 的远程安装服务中，除了支持 Windows XP Professional 外，还支持 Windows Server 2003 Standard Edition、Windows Server 2003 Web Edition、Windows Server 2003 Enterprise Edition、64 位版本的 Windows Server 2003 Enterprise Edition、Windows 2000 Professional、Windows 2000 Server 和 Windows 2000 Advanced Server 的远程安装。

14.1.2 Windows 部署服务简介

Windows 部署服务是 RIS 服务的升级版，它可以使用“Windows 映像”（WIM）文件安装 Windows 操作系统。当前，Windows 映射文件格式包括 Windows Vista 和 Windows Server 2008 操作系统，即 Windows 部署服务可以用来安装 Windows Vista 和 Longhorn 操作系统。

Windows 部署服务包含一台 PXE 服务器和一台普通文件传输协议 (TFTP) 服务器，并包含一个客户端界面和一个管理单元。

14.2 远程安装服务的系统需求

远程安装服务主要在企业网络中使用，对使用环境具有一定的要求。例如对服务器的硬件要求。客户端必须使用 PXE 网卡，必须使用其活动目录的网络等。

►► 14.2.1 服务需求

远程安装服务需要如下组件的支持。

- (1) 动态主机配置协议 (DHCP)：用于为客户端分配 IP 地址。
- (2) 域名系统 (DNS)：实现域名解析功能。
- (3) Active Directory：为客户端提供用户认证服务，在实际使用中可以将 DHCP、DNS 和 Active Directory 与 RIS 安装在一台或多台服务器中。
- (4) 远程启动技术 RIS：使用远程启动技术允许没有操作系统的计算机从网络适配器开始启动过程，启动后可以从网络安装操作系统。另外，如果客户端没有 PXE 引导芯片，也可以使用特别的远程启动盘（如果具有支持的网络适配器）。
- (5) 创建安装映像的技术：包括可用于创建要在客户端中安装的操作系统映像的技术。
- (6) 在 RIS 客户端和服务端间通信的技术：RIS 包括在开始 PXE 启动过程的客户端和 RIS 服务器（包括可用于该客户端的安装映像）间建立通信的技术。对于该过程，RIS 使用 DHCP 向客户端提供 Internet 协议 (IP) 地址，然后下载“客户端安装向导”。该向导将提示用户登录并提供为该用户自定义的安装选项菜单，通过“组策略”可控制这些映像。
- (7) 远程安装 (BINLSVC)：该服务侦听客户端的网络服务请求并且提供 RIS 环境的全面管理，以确保正确的文件能传送到客户端。
- (8) 日常文件传输协议守护程序 (TFTPD)：RIS 服务器使用该程序下载开始远程安装过程所需的初始文件，使用 TFTPD 下载到客户端的最常见的文件是 Startrom.com，它负责启动客户端计算机。
- (9) 单一实例存储 (SIS)：减少了 RIS 卷中所需要的总存储量。SIS 驱动程序包括一个称为“文件签名比较服务代理”的功能，它可以扫描 RIS 卷中的重复文件。如果 SIS 文件签名比较服务发现了重复的文件，则将原始文件复制到 SIS，并且在原来的位置留下一个链接文件。

►► 14.2.2 服务器硬件需求

1. 基于 x86 的计算机的需求

- (1) 建议使用最小速度为 550 MHz（最小速度为 133 MHz）的一个或多个处理器。每台计算机最多支持 8 个处理器。建议使用 Intel Pentium/Celeron 系列、AMD K6/Athlon/Duron 系列或兼容处理器。
- (2) 建议最少 256 MB RAM（最小支持 128 MB，最大支持 32 GB）。
- (3) 对于 RAM 大于 4 GB 的计算机，需通过硬件兼容性验证。

2. 基于 Itanium 体系结构的计算机需求

- (1) 建议使用最小速度为 733 MHz 的一个或多个处理器。每台计算机最多可支持 8 个处理器。
- (2) RAM 最小为 1 GB，最大为 64 GB。
- (3) 对于 RAM 大于 4 GB 的计算机，需通过硬件兼容性验证。

3. 确保具有足够可用空间

为了确保以后使用操作系统时具有灵活性，建议可用空间设置为比运行安装程序所要求的最小空

间大。若是在基于 x86 的计算机上, 该空间大约为 1.25 GB~2 GB; 在基于 Itanium 体系结构的计算机上为 3 GB~4 GB。如果通过网络, 不是通过光盘运行安装程序, 或者正在 FAT 或 FAT32 分区 (NTFS 是建议的文件系统) 上安装, 则需要更大的空间。

4. 网卡

使用支持 TCP/IP 的 10 Mb/s 或 100 Mb/s Windows 兼容的网络适配器, 如果条件允许, 建议使用更高速度的网卡。另外作为 RIS 服务器, 只能使用一块网卡, 而不能同时使用多块。

14.2.3 客户端需求

客户端必须满足要安装的操作系统的最低要求。

PXE 基于 DHCP 的启动 ROM 的版本为 1.00 或更高版本。如果没有 PXE 的引导芯片, 必须为计算机创建引导软盘, 并且用 rbfq.exe 程序生成一张启动软盘。

14.2.4 其他考虑事项

其他考虑事项如下。

- (1) 因为需要保存客户操作系统安装文件, 所以 RIS 需要大量的磁盘空间。
- (2) RIS 不能安装在与系统卷或启动卷相同的分区中。
- (3) 用来安装 RIS 的卷必须使用 NTFS 文件系统格式化。
- (4) RIS 不支持加密文件系统 (EFS), 以及“分布式文件系统” (DFS) 作为目标位置, 但是可在运行 DFS 的计算机上同时运行 RIS。

14.2.5 远程安装服务的前期准备

在 Windows XP 中远程安装服务之前, 需要确保完成如下工作。

- (1) 在网络中安装 Windows 2000、Windows Server 2003 或者 Windows Server 2008 服务器, 并且将其升级到 Active Directory 的域控制器。
- (2) 在网络中安装 DHCP 服务器, 创建合法的作用域并且将其激活。
- (3) DHCP 服务器已经在 Active Directory 服务器中授权。
- (4) 在网络中安装 DNS 服务器, 并进行相关的配置。通常情况下, 此 DNS 服务器与 Active Directory 服务器是同一台机器。
- (5) 作为 RIS 的服务器, 必须是 Active Directory 的成员服务器, 网络中可以有一台或多台 RIS 服务器。
- (6) 如果网络拥有多个 VLAN, 需要在“中心交换机”上配置“DHCP 中继代理”。并且将 RIS 服务器的 IP 地址添加到“DHCP 中继代理”中, 这样 RIS 服务器才能跨子网使用。

如果只是为了做实验, 则可以将 RIS 服务器、Active Directory 域控制器、DNS 和 DHCP 服务器安装在一台机器上; 如果是在企业应用中, RIS 服务器和 DHCP 服务器必须独立, Active Directory 域控制器与 DNS 服务器可以集成在一起, 如图 14-1 所示。

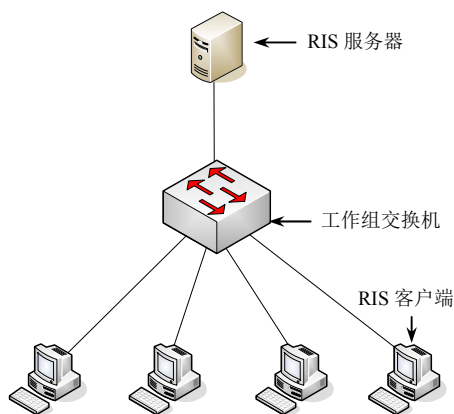


图 14-1 RIS 服务器

14.3 RIS 远程安装服务实现步骤

为实现操作系统的远程安装, 首先需要做好前期准备工作。即将网络升级到域环境, 同时在域控制器上安装 DHCP 和 DNS 服务。

14.3.1 安装 RIS 服务器

在 Windows Server 2003 的服务器中安装 DHCP 服务器，升级 Windows Server 2003 到 Active Directory 服务器，并以系统管理员身份登录到这台服务器。

1. 添加 RIS 远程安装服务

① 单击“开始”→“控制面板”→“添加/删除程序”选项，显示如图 14-2 所示的“添加或删除程序”窗口。

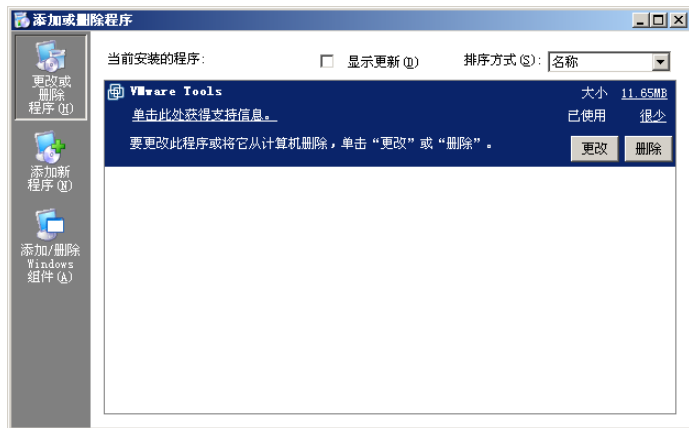


图 14-2 “添加或删除程序”窗口

② 单击“添加/删除 Windows 组件”按钮，显示如图 14-3 所示的“Windows 组件向导”对话框，在“组件”下标列表框中选中“远程安装服务”复选框。

③ 单击“下一步”按钮，安装程序将开始复制文件。安装过程中，安装程序会提示插入 Windows Server 2003 的安装光盘，如图 14-4 所示，将 Windows Server 2003 的安装光盘插入光驱即可。



图 14-3 “Windows 组件向导”对话框

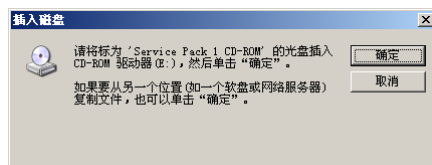


图 14-4 提示插入 Windows Server 2003 安装光盘

④ 安装完成后，显示如图 14-5 所示的“完成‘Windows 组件向导’”对话框。

⑤ 单击“完成”按钮，完成 RIS 服务的安装。显示如图 14-6 所示的“系统设置改变”对话框，提示需要重新启动计算机才能使设置生效。

⑥ 单击“是”按钮重新启动计算机。

2. 复制 Windows XP 的安装文件到 RIS 服务器

虽然成功安装了 RIS 服务，但因为此时 RIS 服务器中并没有客户端操作系统的安装文件，所以还不能为其安装操作系统，需要将客户端操作系统的安装文件导入到 RIS 服务器中。

① 重新启动 Windows Server 2003，打开如图 14-7 所示的“运行”对话框，在“打开”下拉列表

框中键入 risetup。

- ② 单击“确定”按钮，显示如图 14-8 所示的“远程安装服务安装向导”对话框。



图 14-5 “完成 ‘Windows 组件向导’” 对话框

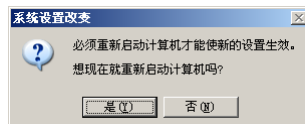


图 14-6 提示重新启动计算机

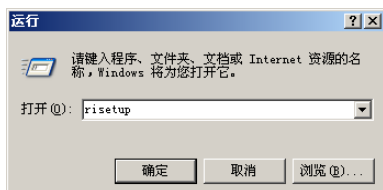


图 14-7 “运行” 对话框

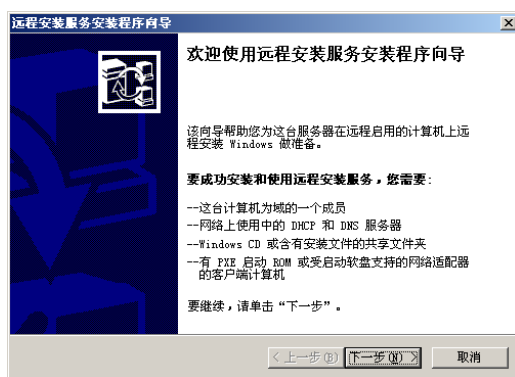


图 14-8 “远程安装服务安装向导” 对话框

③ 单击“下一步”按钮，显示如图 14-9 所示的“远程安装文件夹的位置”对话框。单击“浏览”按钮，设置保存 Windows XP 安装文件目录的对话框。需要注意的是，这里所设置的磁盘必须使用 NTFS 文件系统，并且拥有足够大的空闲空间。

④ 单击“下一步”按钮，显示如图 14-10 所示的“初始设置”对话框。在其中可以控制远程安装服务器与客户端相互作用的方法，如果选中“响应客户端计算机的请求服务”复选框，则在设置完成后会立即响应客户端计算机。这里保持默认设置，即清除该复选框。

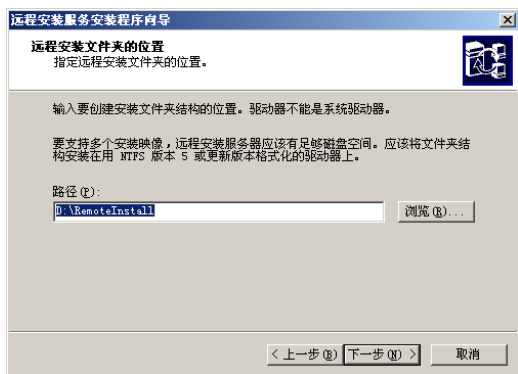


图 14-9 选择保存 Windows XP 的目录

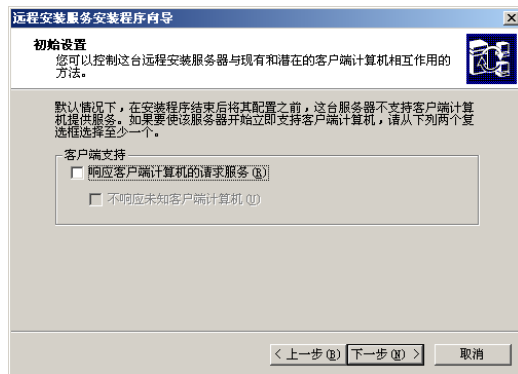


图 14-10 “初始设置” 对话框

⑤ 单击“下一步”按钮，显示如图 14-11 所示的“安装源文件的位置”对话框。单击“浏览”按钮，浏览 Windows XP Professional 安装源文件目录。

⑥ 单击“下一步”按钮，显示如图 14-12 所示的“Windows 安装映像文件夹名称”对话框。在“文件夹名”文本框中输入复制 Windows 安装映像的目标文件夹名称，默认名称为“WINDOWS”。

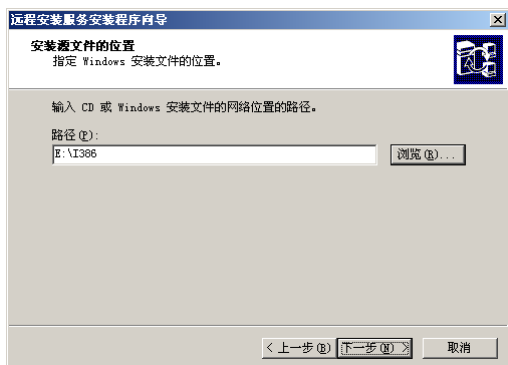


图 14-11 “安装源文件的位置”对话框

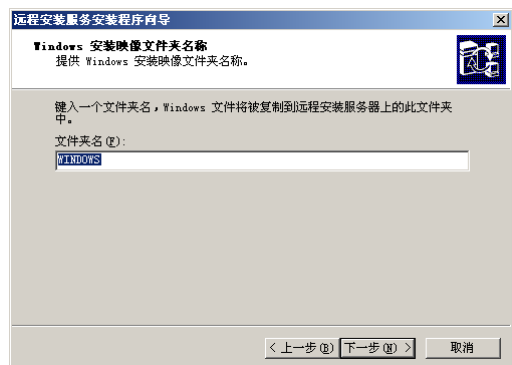


图 14-12 “Windows 安装映像文件夹名称”对话框

⑦ 单击“下一步”按钮，显示如图 14-13 所示的“易懂描述和帮助文字”对话框。为该安装映像设置一个易懂的描述和帮助文字，在“易懂描述”文本框中输入该安装映像的描述信息，在“帮助文字”文本框中输入该安装映像的帮助文字。

⑧ 单击“下一步”按钮，显示如图 14-14 所示的“复查设置”对话框。检查设置是否正确，单击“上一步”按钮，可以返回重新设置。

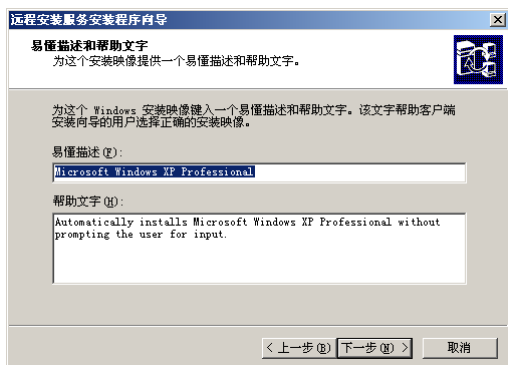


图 14-13 “易懂描述和帮助文字”对话框

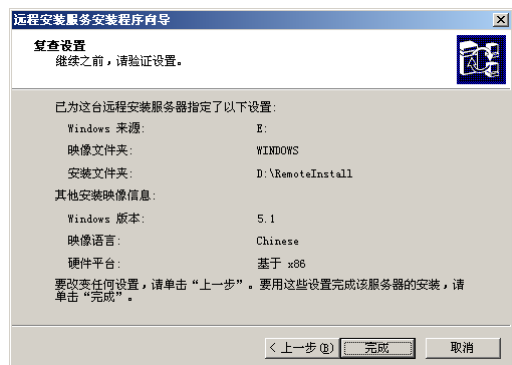


图 14-14 “复查设置”对话框

⑨ 检查无误后，单击“完成”按钮，即可配置和复制 Windows XP Professional 的安装源文件。RIS 服务配置完成后，显示如图 14-15 所示的提示框。

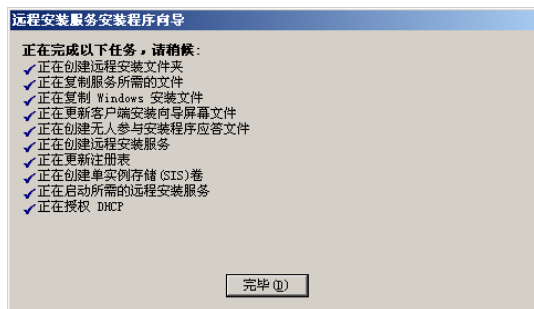


图 14-15 提示框

⑩ 单击“完成”按钮，完成客户端系统映像的复制操作。

14.3.2 授权 RIS 服务器

Windows Server 2003 的 DHCP 服务器必须经过授权才能正常使用，但在 RIS 服务器安装并复制

Windows XP 的安装文件后, RIS 服务器会自动完成 DHCP 服务器的授权。因此在 Windows Server 2003 中, 不再需要单独授权 DHCP 服务器, 如图 14-16 所示。

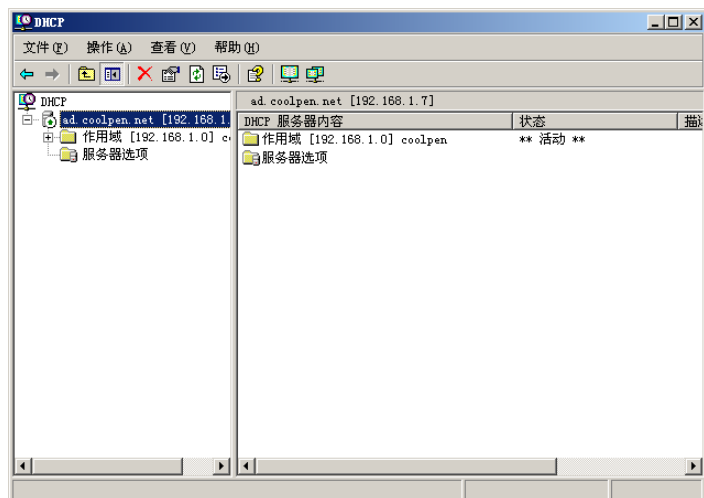


图 14-16 不再需要单独授权 DHCP 服务器

14.3.3 配置 RIS 服务器

为 RIS 服务器授权后, 还需要配置 RIS 服务器, 操作步骤如下。

① 单击“开始”→“管理工具”→“Active Directory 用户和计算机”选项, 打开如图 14-17 所示“Active Directory 用户和计算机”窗口, 如图 14-17 所示。

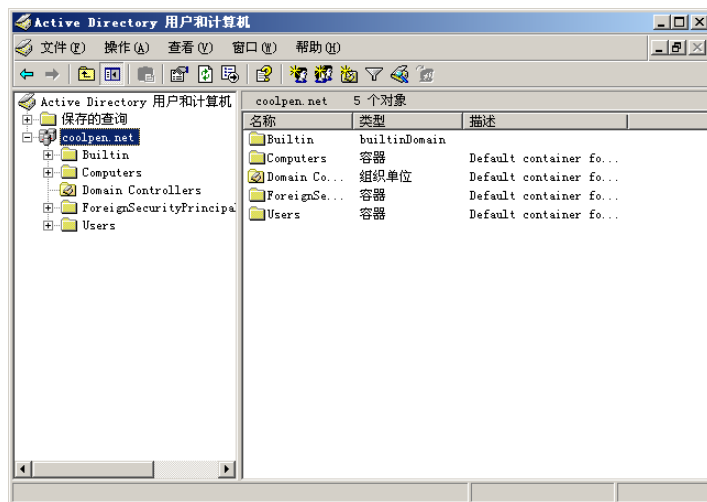


图 14-17 “Active Directory 用户和计算机”窗口

② 在左侧窗格中选择“Domain Controllers”选项, 在右边的窗格中将列出当前网络中的所有域控制器。右击相应的 RIS 服务器, 在快捷菜单中选择“属性”选项, 显示如图 14-18 所示的“AD 属性”对话框。

③ 打开到如图 14-19 所示的“远程安装”选项卡, 选中“响应客户端计算机的请求服务”复选框, RIS 服务器即可开始为发出响应的 RIS 客户端提供服务。

提示

单击“验证服务器”按钮, 可以检查 RIS 服务器是否有故障。

④ 单击“应用”按钮保存设置。

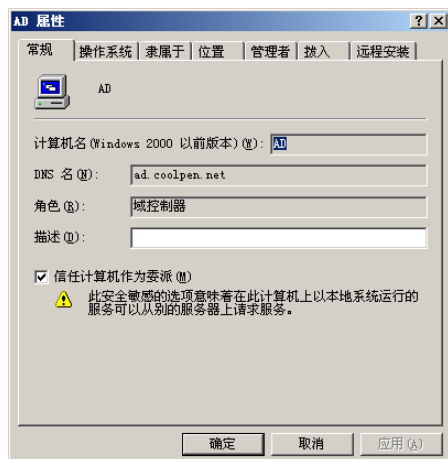


图 14-18 “AD 属性”对话框

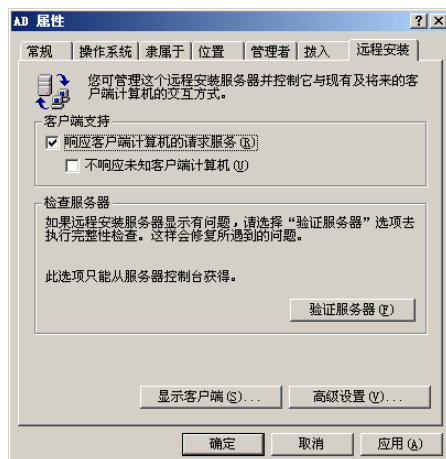


图 14-19 “远程安装”选项卡

14.3.4 禁止 RIS 安装过程中重新分区硬盘

在默认情况下，RIS 服务只提供全新的安装。如果硬盘已经分区，在用默认的 RIS 服务安装时，远程安装服务将会自动格式化硬盘，并把硬盘划分为一个分区。这种情况只适合安装全新的计算机。为了适应已经分区的计算机安装操作系统，需要完成如下配置。

① 在“AD 属性”对话框中打开“远程安装”选项卡，单击“高级设置”按钮，显示“AD-Remote-Installation-Services 属性”对话框，打开如图 14-20 所示的“映像”选项卡。

② 单击“添加”按钮，显示如图 14-21 所示的“新的应答文件或安装映像”对话框。选择“将新的应答文件与一个现有映像联系起来”单选按钮，将一个全新且无人参与的安装应答文件复制为现有的映像。



图 14-20 “映像”选项卡

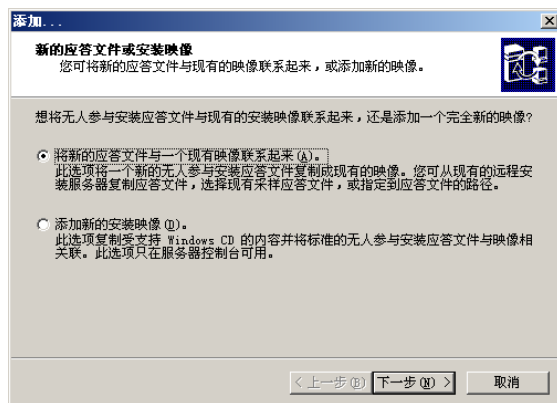


图 14-21 “新的应答文件或安装映像”对话框

③ 单击“下一步”按钮，显示如图 14-22 所示的“无人参与的安装应答文件源”对话框，在“选择要复制的无人参与安装应答文件资源”选项组中选择“Windows 映像采样文件”单选按钮。

④ 单击“下一步”按钮，显示如图 14-23 所示的“选择安装映像”对话框。指定需要与无人参与安装应答文件相关联的安装映像，在列表框中选择已经存在的安装映像。

⑤ 单击“下一步”按钮，显示如图 14-24 所示的“选择示例应答文件”对话框，选择应答文件的“Windows Professional-no repair”选项。

⑥ 单击“下一步”按钮，显示如图 14-25 所示的“易懂描述和帮助文字”对话框。为 RIS 远程安装服务输入描述信息文字，分别在“易懂描述”和“帮助文字”文本框中输入相应的易懂描述和帮

助文字即可。

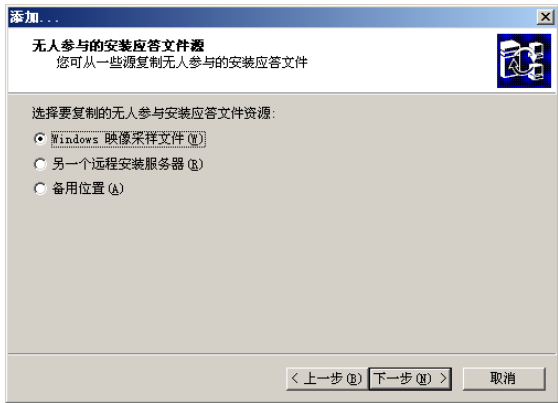


图 14-22 “无人参与的安装应答文件源”对话框



图 14-23 “选择安装映像”对话框

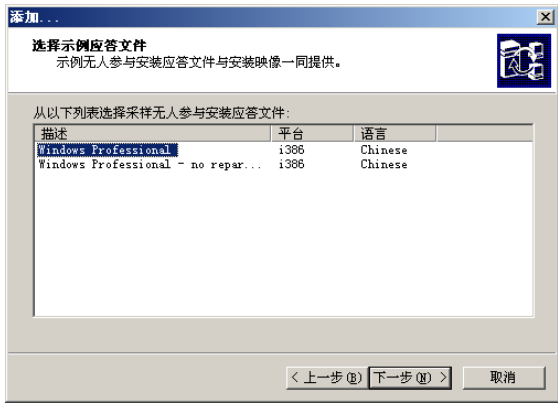


图 14-24 “选择示例应答文件”对话框

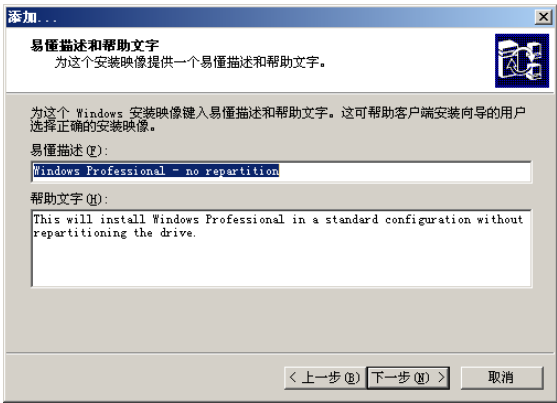


图 14-25 “易懂描述和帮助文字”对话框

- ⑦ 单击“下一步”按钮，显示如图 14-26 所示的“复查设置”对话框。检查设置是否正确，并记录“目标路径”文本框中的网络路径信息。
- ⑧ 单击“完成”按钮，完成设置并返回“AD 属性”对话框，如图 14-27 所示。

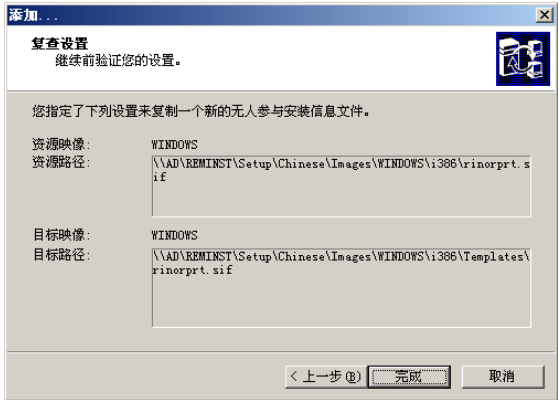


图 14-26 “复查设置”对话框

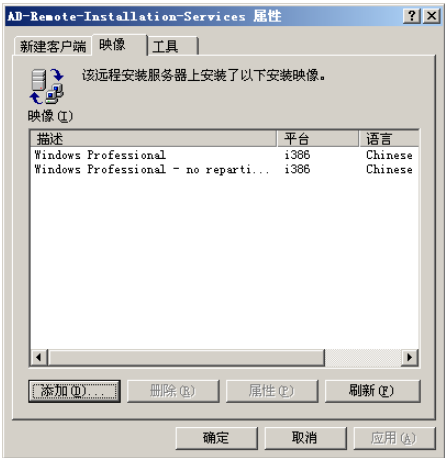


图 14-27 “AD 属性”对话框

- ⑨ 单击“确定”按钮，保存设置并返回“Active Directory 用户和计算机”窗口。
- ⑩ 打开“目标路径”中的网络路径，并使用记事本打开 rinorprt.sif 文件，其内容如图 14-28 所示。

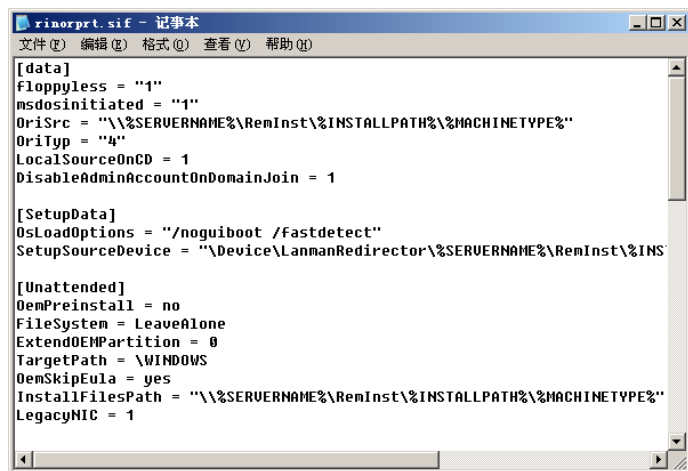


图 14-28 rinorprt.sif 文件内容

⑪ 查找如下内容：

```
[RemoteInstall]
Repartition = Yes
UseWholeDisk = Yes
```

将其修改为如下内容：

```
[RemoteInstall]
Repartition = No
```

⑫ 单击“开始”→“保存”选项，保存修改。

14.3.5 自动完成 RIS 远程安装系统

如果需要 RIS 在远程安装操作系统的过程中自动输入产品的序列号及加入域等操作，还需要如下修改配置文件。

在文件中查找如下内容：

```
[Unattended]
OemPreinstall = no
FileSystem = LeaveAlone
ExtendOEMPartition = 0
TargetPath = \WINDOWS
OemSkipEula = yes
InstallFilePath = "\\%SERVERNAME%\RemInst\%INSTALLPATH%\%MACHINETYPE%"
LegacyNIC = 1
```

将其修改为：

```
[Unattended]
OemPreinstall = no
FileSystem = LeaveAlone
ExtendOEMPartition = 0
TargetPath = \WINDOWS
OemSkipEula = yes
InstallFilePath = "\\%SERVERNAME%\RemInst\%INSTALLPATH%\%MACHINETYPE%"
LegacyNIC = 1
UnattendMode=DefaultHide
NtUpgrade=No
OverwriteOemFilesOnUpgrade=No
```

在文件中查找如下内容：

```
[UserData]
FullName = "%USERNAME%"
OrgName = "%ORGNAME%"
ComputerName = %MACHINENAME%
```

将其修改为:

```
[UserData]
FullName = "%USERFIRSTNAME% %USERLASTNAME%"
ComputerName = %MACHINENAME%
ProductKey=11114-22222-33333-44444-55555 //远程安装操作系统的序列号
OrgName="衡水学院"
```

在文件中查找以下内容:

```
[Identification]
JoinDomain = %MACHINEDOMAIN%
DoOldStyleDomainJoin = Yes
```

将其修改为:

```
[Identification]
JoinDomain = coolpen.net //RIS 当前所在的域
DoOldStyleDomainJoin = Yes
```

修改完成后,保存设置并退出。如果需要修改另一个配置文件,需要修改同一目录下的 ristndrd.sif 文件。该文件与上述文件类似,只是在安装过程中要将硬盘创建成一个分区并格式化。此配置文件只用于新硬盘的安装,建议管理员将其删除。

►► 14.3.6 允许远程安装

设置允许远程安装的操作步骤如下。

- ① 在“Active Directory 用户和计算机”窗口中右击域名,在快捷菜单中选择“属性”选项,显示如图 14-29 所示的“coolpen.net 属性”对话框。
- ② 打开如图 14-30 所示的“组策略”选项卡,在策略列表框中选中默认的策略。

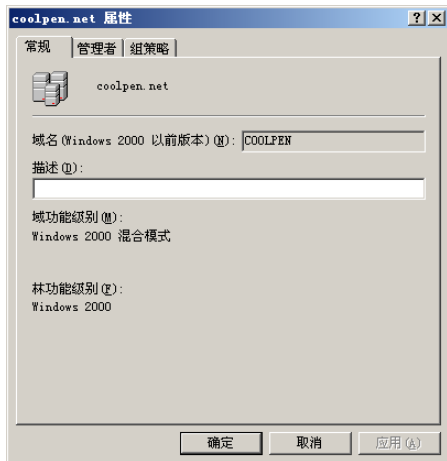


图 14-29 “coolpen.net 属性”对话框

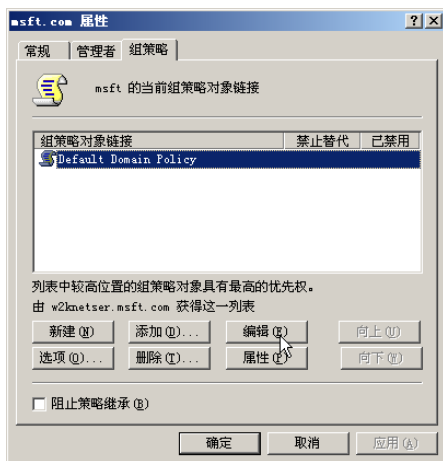


图 14-30 “组策略”选项卡

- ③ 单击“编辑”按钮,打开如图 14-31 所示的“组策略编辑器”窗口,展开“用户配置”→“Windows 设置”→“远程安装服务”选项。
- ④ 右击“选择选项”图标,在快捷菜单中选择“属性”选项。显示如图 14-32 所示的“选择选项 属性”对话框,将 4 个选项全部设置为“已启用”。

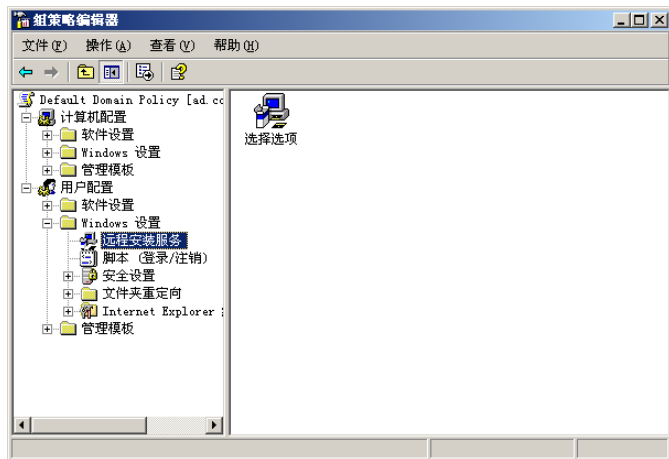


图 14-31 “组策略编辑器”窗口

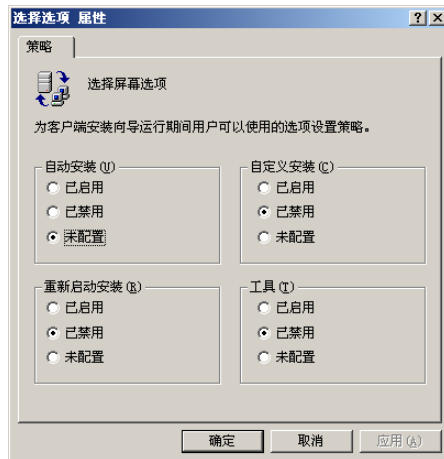


图 14-32 “选择选项 属性”对话框

⑤ 单击“确定”按钮，保存设置。然后关闭默认策略，返回到“Active Directory 用户和计算机”窗口。

14.3.7 委派所有用户可以将计算机加入到域

如果想让每个用户都能自行将计算机加入到域，还需要委派每个用户组具有把计算机加入到域的权限，操作步骤如下。

① 在“Active Directory 用户和计算机”窗口中右击域名，在快捷菜单中选择“委派控制”选项，显示如图 14-33 所示的“控制委派向导”对话框。

② 单击“下一步”按钮，显示如图 14-34 所示的“用户和组”对话框。

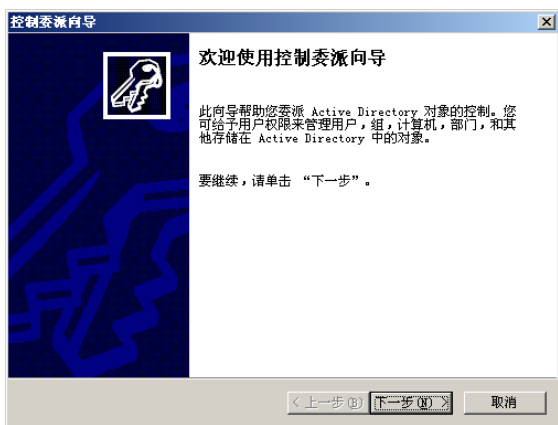


图 14-33 “控制委派向导”对话框



图 14-34 “用户和组”对话框

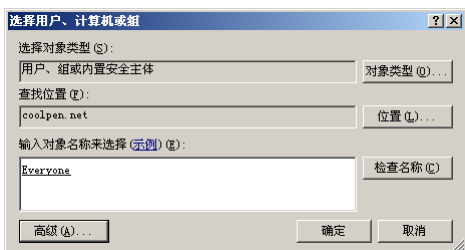


图 14-35 “选择用户、计算机和组”对话框

③ 单击“添加”按钮，显示如图 14-35 所示的“选择用户、计算机和组”对话框，在“输入对象名称来选择”文本框中输入 Everyone。

④ 单击“确定”按钮，显示如图 14-36 所示的“要委派的任务”对话框，选中“将计算机加入到域”复选框。

⑤ 单击“下一步”按钮，显示如图 14-37 所示的“完成控制委派向导”对话框。

⑥ 单击“完成”按钮完成委派控制。

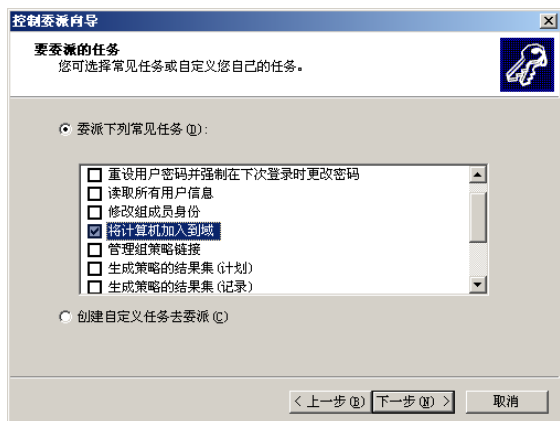


图 14-36 “要委派的任务”对话框

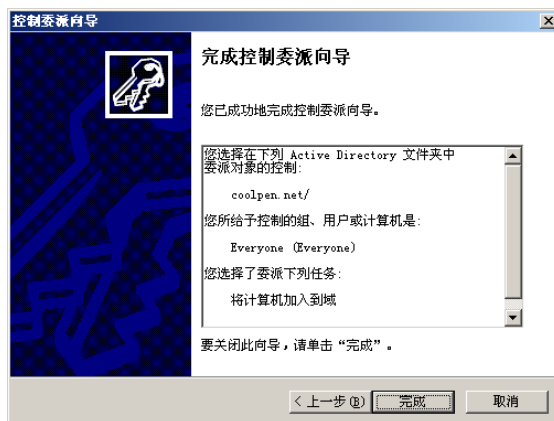


图 14-37 “完成控制委派向导”对话框

14.4 实现远程安装服务

服务器设置完成后，客户端即可开始使用 RIS 服务器安装操作系统，这里以客户端安装 Windows XP Professional 为例介绍。

14.4.1 远程安装对客户端的需求

远程安装服务对于客户端要求如下。

- (1) 满足客户端操作系统的最低系统要求。
- (2) 安装具有 PXE 功能的网卡。

14.4.2 创建引导软盘

如果客户端已经安装了支持 PXE 的网卡，但是没有 PXE 的芯片，则可以利用 RBFPG 程序创建一张软盘。用这张软盘引导，也可以代替网卡的启动芯片。需要说明的是，用 RBFPG 生成的软盘只支持如下型号的网卡。

- (1) 3COM 3C900B-Combo。
- (2) 3COM 3C900B-FL。
- (3) 3COM 3C900B-TPC。
- (4) 3COM 3C900B-TPO。
- (5) 3COM 3C900-Combo。
- (6) 3COM 3C900-TPO。
- (7) 3COM 3C905B-FX。
- (8) 3COM 3C905B-TX。
- (9) 3COM 3C905C-TX。
- (10) 3COM 3C905-T4。
- (11) 3COM 3C905-TX。
- (12) AMD PCnet Adapters。
- (13) Compaq NetFlex100。
- (14) Compaq NetFlex110。
- (15) Compaq NetFlex3。
- (16) DEC DE450。
- (17) DEC DE500。

- (18) HD DeskDirect 10/100 TX。
- (19) Intel Pro 10+。
- (20) Intel Pro 100+。
- (21) Intel Pro 100B。
- (22) SMC 8432。
- (23) SMC 9332。
- (24) SMC 9432。

如果所用网卡不在上述列表中，并要使用 RIS 安装，必须要有 PXE 的启动芯片。

RBFG 程序保存在 Windows XP Professional 安装光盘的\RemoteInstall\Admin\i386 目录下，在其中双击 rbfq.exe 程序，显示如图 14-38 所示的“Microsoft Windows 远程启动磁盘生成器”对话框。

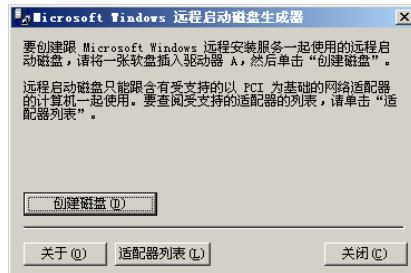


图 14-38 “Microsoft Windows 远程启动磁盘生成器”对话框

找一张质量比较好的磁盘放在软驱中，单击“创建磁盘”按钮即可生成远程启动磁盘。使用这张软盘可以实现远程安装的功能。

14.4.3 在客户端中安装 Windows XP Professional

如果使用的客户端已经配置了 PXE 的网卡和 PXE 的芯片，就可以使用 RIS 远程安装服务来安装 Windows XP Professional。

(1) 启动客户端，在提示用户使用何种引导方式时按下使用网络引导的按键。显示当前所用网卡的版本等信息，如图 14-39 所示。并提示用户按下键盘上的 F12 键，启动网络服务引导。

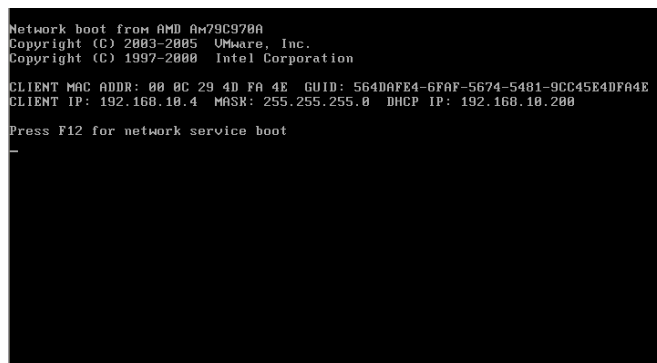


图 14-39 所用网卡的信息

(2) 显示欢迎使用客户端安装向导界面，这个向导可以帮助用户快速并且简单的安装操作系统，并且可以始终使用该向导来更新和修复计算机。在该界面中，要求使用网络中的有效用户名、密码和域名称，如果用户没有这些信息，则联系网络管理员获取。然后按回车键继续，如图 14-40 所示。

(3) 按回车键，显示如图 14-41 所示的登录信息设置。按 TAB 键在各选项之间进行切换，并输入有效的用户名、密码和域名称。如果要清除所输入的信息，则按 Esc 键即可。确认输入的信息正确后，按回车键继续。

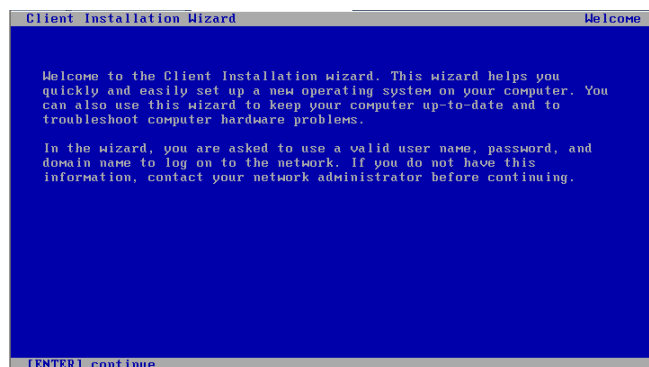


图 14-40 客户端安装向导

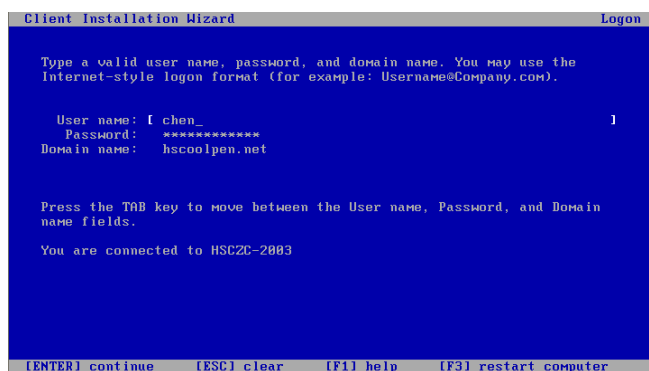


图 14-41 登录信息设置

(4) 显示如图 14-42 所示的主菜单，可以根据用户的实际需要选择，其中包括如下 4 个选项。

- **Automatic Setup:** 自动安装方式，这是最简单的安装方式。网络管理员已经设置其中的多个选项，因此不需要用户设置。
- **Custom Setup:** 自定义安装方式，使用该方式用户可以设置自己的计算机名称等信息。
- **Restart a Previous Setup Attempt:** 重新启动计算机，继续先前已经开始的系统安装。
- **Maintenance and Troubleshooting:** 选择该选项可以更新和修复当前系统。

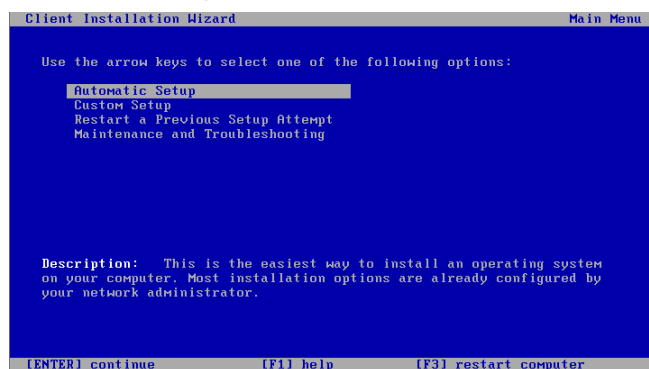


图 14-42 主菜单

选择安装选项后，按回车键继续操作。这里我们选择第 1 项。如果此时按下 F3 键，还可以重新启动计算机。

(5) 在系统选项窗口中，选择准备安装的操作系统，如图 14-43 所示。

- **Windows Professional – no repartition:** 该选项不会自动将整个硬盘分成一个区。
- **Windows Professional:** 安装 Windows XP 专业版的标准配置。

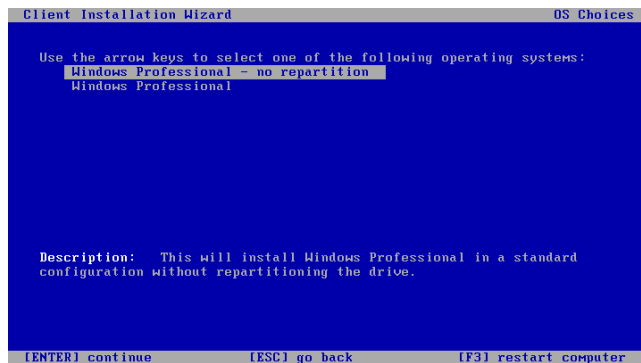


图 14-43 系统选项窗口

这里我们选择第 1 项，按回车键继续，按 Esc 键可以返回上一个窗口。

(6) 系统警告用户，在系统安装之前必须分区和格式化硬盘，如图 14-44 所示。如果该硬盘已经分区和格式化，一旦开始安装系统，将会把硬盘中现有的数据全部删除。按回车键继续，如果要中止操作，按 Esc 键即可。

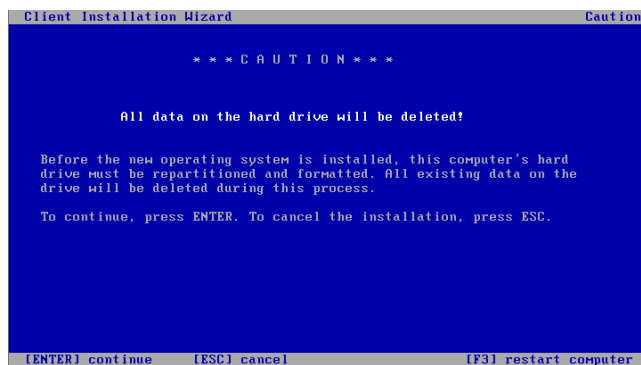


图 14-44 警告

(7) 在如图 14-45 所示的安装信息窗口中显示安装信息，包括计算机名称、ID 信息及安装该操作系统的服务器名称。按回车键即可开始安装系统。另外，在开始安装系统之前，如果软驱和光盘中有磁盘，必须将其取出。

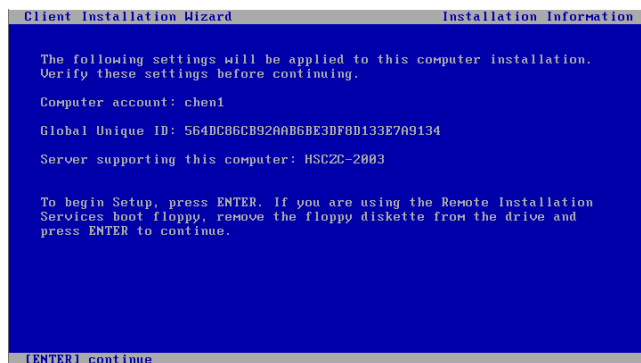


图 14-45 “安装信息”窗口

(8) 按回车键，开始安装 Windows XP，使用这种安装方式安装的操作系统与使用光盘安装的操作系统完全一样。

14.5 安装与配置 Windows 部署服务

Windows 部署服务 (Microsoft Windows Deployment Services, WDS) 是快速远程部署 Windows

操作系统的一种方法，例如部署 Windows Vista 或 Windows Server 2008。该服务允许用户通过网络在未安装操作系统的计算机中安装 Windows 操作系统，而不需要用户直接操作目标计算机。在 Windows Server 2003 中，Windows 部署服务曾作为一个更新被推出，但在 Windows Server 2008 中则作为一个系统组件被集成到系统安装光盘中。

14.5.1 Windows 部署服务组件

Windows 部署服务包含以下 3 个组件。

(1) 服务器组件：用于网络启动客户端的 PXE 服务器和 TFTP 服务器，以加载并安装操作系统。在组件中还包括一个共享文件夹和映像存储库，其中包含网络启动所需要的启动映像、安装映像及文件。

(2) 客户端组件：主要包括一个图形用户界面，该界面与 Windows Server 2003 中的 RIS 完全不同，而是一个全新且更加人性化的图形界面。客户端组件与服务器组件通信，以供选择和安装操作系统映像。使用客户端组件，也可以捕获已安装好的计算机操作系统。并且还可以将其存储在光盘中，以在不支持 PXE 的计算机上使用。

(3) 管理组件：包括 WDS 管理控制台和命令行工具，用于管理服务器、操作系统映像和客户端计算机账户。

14.5.2 Windows 部署服务的优点

Windows 部署服务拥有很多优点，使得在企业应用中能够有效降低手动安装效率低下所带来的相关成本。并且提高了操作系统和应用程序的性能一致性，减少了管理员在手动安装时所咨询的次数，同时还减少了安装操作系统和常用应用程序所耗费的时间。

Windows 部署服务客户端依赖 Windows PE 提供启动服务和部署，这是与 RIS 所不同的。Windows 部署服务提供了简单易用的菜单，并提供与 Windows 安装程序相同的安装过程。如果在部署中出现問題，可以通过快捷键来调用命令行状态排错和分析。

14.5.3 服务器的功能模式

Windows 部署服务有两种安装方式，一种是在 RIS 的基础上升级安装；一种是全新安装。使用不同的安装方式，Windows 部署服务所采用的服务器模式也不同，具体包括以下 3 种模式，即旧模式、混合模式和纯模式。

1. 旧模式

旧模式的 Windows 部署服务在功能上与远程安装服务（RIS）相同，从某种意义上来说，它是具有 RIS 功能的 Windows 部署服务二进制文件。在该模式下，启动操作系统只能由 OSChooser 来完成。换句话说，只能使用 RISETUP 和 RIPREP 映像。从管理的难易程度来看，建议使用 Windows Server 2003 服务器中的 RIS 管理工具。

2. 混合模式

Windows 部署服务混合模式主要是用来描述服务器状态，在该状态下可以使用 OSChooser 和 Windows PE 两种启动映像，通过 OSChooser 可以使用 RISETUP 和 RIPREP 映像；通过 Windows PE 启动映像则可以使用 WIM 格式的启动映像。混合模式的优点是在启动菜单中可以选择进入 RIS 或 Windows PE；在管理性上，可以使用旧版管理工具管理 RISETUP 和 RIPREP 映像，使用新版 Windows 部署服务管理工具管理 WIM 映像。需要注意的是，Windows 部署服务混合模式只能安装于 Windows Server 2003 上。

3. 纯模式

Windows 部署服务纯模式指仅支持 Windows PE 启动映像的 Windows 部署服务服务器，该模式既

可以安装在 Windows Server 2003 服务器上，也可以安装在 Windows Server 2008 服务器上。但需要注意的是，在 Windows Server 2008 服务器上只能安装 Windows 部署服务的纯模式。在纯模式下，只能部署 WIM 映像到客户端，并且服务器的管理只能使用新版的 Windows 部署服务管理工具。

14.5.4 Windows 部署服务的要求

1. 系统需求

Windows 部署服务的要求相对于 RIS 来说要苛刻得多，该服务包含对服务器操作系统和网络环境的要求。首先操作系统必须是 Windows Server 2008、Windows Server 2003 with SP1 或 Windows Server 2003 R2。需要注意的是，微软已经推出了适于 Windows Server 2003 SP1 的 WDS 更新包。如果在 Windows Server 2003 系统中安装 Windows 部署服务，必须首先安装 RIS，但并不需要配置。如果安装了 Windows Server 2003 SP2，并且已经安装过 RIS，则可以直接安装 Windows 部署服务。

其次，网络环境必须满足如下要求。

(1) 动态主机配置协议 (DHCP)。

(2) 域名系统 (DNS)。

(3) Active Directory: 使用 Windows 部署服务时，Active Directory 是必需的，而且 DHCP、DNS 和 Active Directory 可以与 Windows 部署服务安装在一台服务器或多台服务器中。

(4) 远程启动技术: Windows 部署服务使用远程启动技术允许没有操作系统的计算机从网络适配器开始启动过程，启动后可以从网络安装操作系统。如果计算机没有 PXE 的引导芯片，只要有支持的网络适配器，用户也可以使用特别的远程启动盘。

(5) 创建安装映像的技术: Windows 部署服务包括可用于创建要在客户端上安装的操作系统映像的技术，可使用平面映像或“远程安装准备向导”(RIPrep) 映像格式来创建映像。使用平面映像选项直接从一套操作系统文件中创建映像，例如光盘中的文件；使用 RIPrep 映像格式创建包括具有特定设置和应用程序的操作系统映像，例如，符合某个企业桌面标准的映像。

2. 客户端需求

客户端必须满足要安装的操作系统的最低要求，预启动执行环境的基于 DHCP 的启动 ROM 的版本 2.00 或更高版本。如果没有 PXE 的引导芯片，则需要使用 rbf.exe 程序生成启动软盘来启动计算机。对于部署 Windows Vista 和 Windows Server 2008 系统来说，客户端的内存必须是 512 MB 以上。如果 Windows 部署服务器所使用的是混合模式，即同时支持 WIM Image 和 RIS Image，则 Windows 部署服务仍支持早期版本的部署服务，但建议客户端的内存不小于 128 MB。

14.5.5 安装 Windows 部署服务

在 Windows Server 2008 中安装 Windows 部署服务组件，与安装其他组件的方法基本相同，操作步骤如下。

① 在“服务器管理器”窗口中单击“添加角色”按钮，运行添加角色向导。单击“下一步”按钮，显示如图 14-46 所示的“选择服务器角色”对话框，选中“Windows 部署服务”复选框。

② 单击“下一步”按钮，显示如图 14-47 所示的“Windows 部署服务概述”对话框，其中显示 Windows 部署服务的简介和一些相关的注意事项。

③ 单击“下一步”按钮，显示如图 14-48 所示的“选择角色服务”对话框，根据实际需要选择所要安装的角色服务。

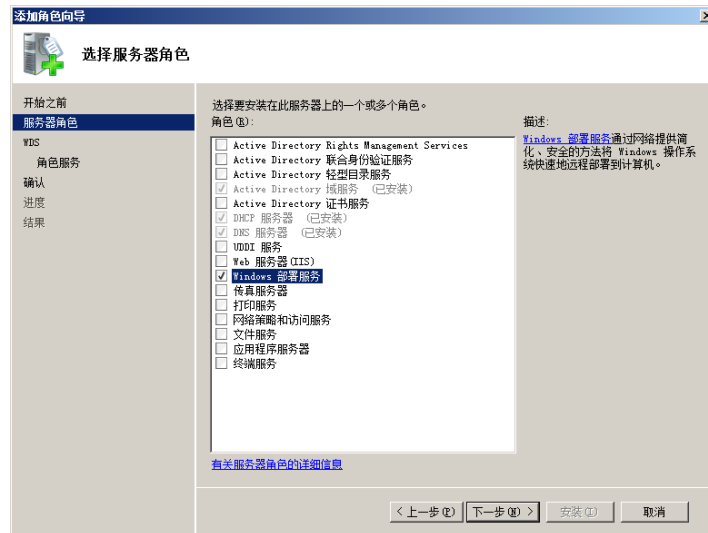


图 14-46 “选择服务器角色”对话框



图 14-47 “Windows 部署服务概述”对话框

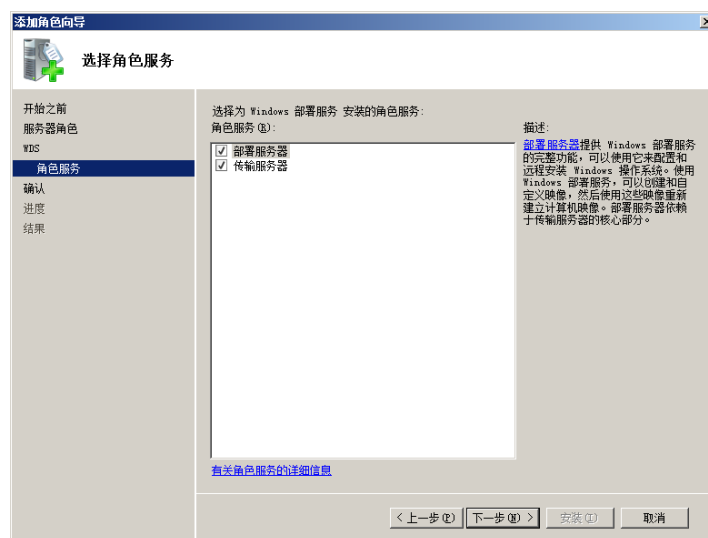


图 14-48 “选择角色服务”对话框

- 部署服务器：该角色服务提供 Windows 部署服务的完整功能，可以用其来配置和远程安装 Windows 操作系统，但部署服务器依赖于传输服务器的核心部分。
 - 传输服务器：该角色服务提供 Windows 部署服务功能的子集，其中只包括核心网络部分，可以使用该部分在独立服务器上使用多播来传输数据。如果使用多播传输数据，而又不希望合并所有 Windows 部署服务，则应选择该角色服务。
- ④ 单击“下一步”按钮，显示如图 14-49 所示的“确认安装选择”对话框。检查所做设置是否正确，单击“上一步”按钮，可以返回重新设置。



图 14-49 “确认安装选择”对话框

- ⑤ 确认无误后，单击“安装”按钮开始安装 Windows 部署服务。安装完成后，显示如图 14-50 所示的“安装结果”对话框，提示 Windows 部署服务安装成功。



图 14-50 “安装结果”对话框

- ⑥ 单击“关闭”按钮，关闭添加角色向导，完成 Windows 部署服务的安装。
- ## ➤➤ 14.5.6 启动 Windows 部署服务

虽然 Windows 部署服务已经成功完成安装，但在默认情况下，Windows 部署服务并不会自动启动，还需要用户进行相关的配置。

① 单击“开始”→“管理工具”→“Windows 部署服务”选项，打开如图 14-51 所示的“Windows 部署服务”窗口。

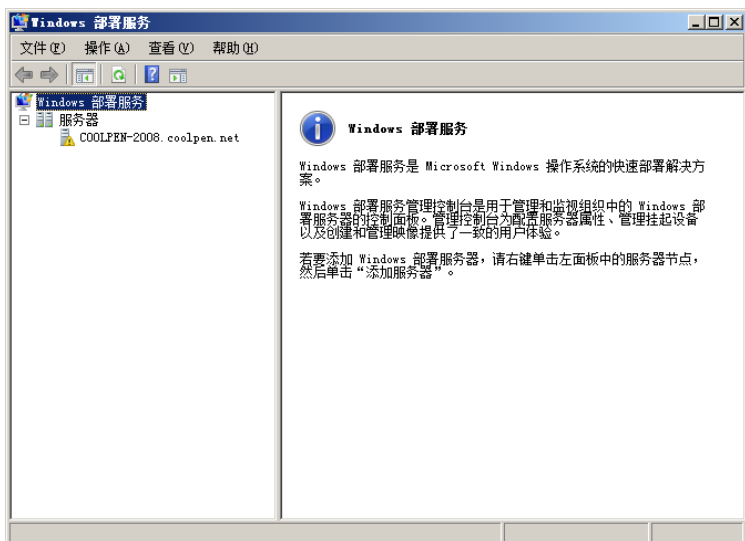


图 14-51 “Windows 部署服务”窗口

② 右击服务器名称，在快捷菜单中选择“配置服务器”选项。启动“Windows 部署服务配置向导”，用来配置 Windows 部署服务。首先显示如图 14-52 所示的“欢迎页面”对话框，提示用户一些需要注意的事项。例如，该计算机必须是 Active Directory 域服务中的成员、网络中存在活动的 DHCP 服务器、网络中存在活动的 DNS 服务器，以及 Windows 部署服务器中用于存储映像的 NTFS 分区等。

③ 单击“下一步”按钮，显示如图 14-53 所示的“远程安装文件夹的位置”对话框。单击“浏览”按钮，浏览并选择待设置的文件夹即可，在远程安装文件夹中包含要从此服务器部署的操作系统映像。需要注意的是，所选择的分区必须具有足够可用空间的 NTFS 分区。

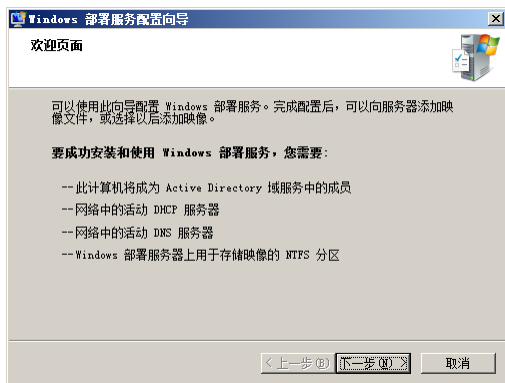


图 14-52 “欢迎页面”对话框

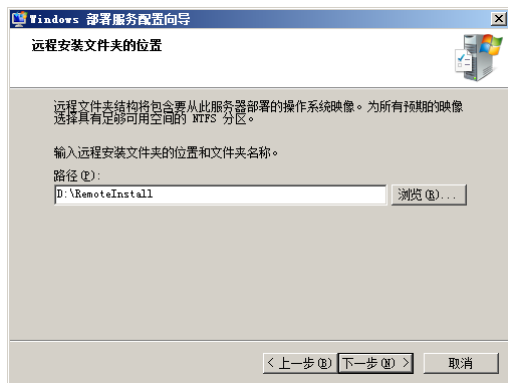


图 14-53 “远程安装文件夹的位置”对话框

④ 单击“下一步”按钮，显示如图 14-54 所示的“DHCP 选项 60”对话框。如果 Windows 部署服务与 DHCP 服务器为同一台计算机，则应选中“不侦听端口 67”和“将 DHCP 选项标记#60 配置为‘PXEClient’”复选框。

⑤ 单击“下一步”按钮，显示如图 14-55 所示的“PXR 服务器初始设置”对话框。预启动执行环境客户可以预留在 Active Directory 域服务中，当客户端已预留时，该计算机称为“已知客户端”；未预留的客户端称为“未知客户端”。根据实际需要，可以选择 Windows 部署服务服务器响应已知和未知客户端时执行的操作。

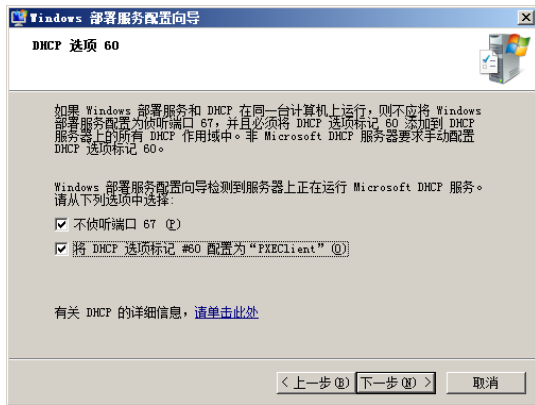


图 14-54 “DHCP 选项 60” 对话框

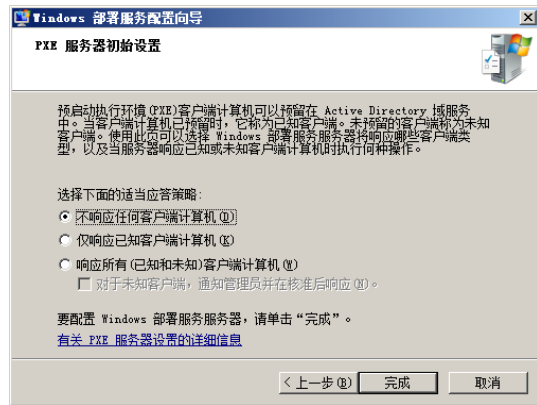


图 14-55 “PXR 服务器初始设置” 对话框

⑥ 单击“完成”按钮，开始启动 Windows 部署服务操作，配置完成后显示如图 14-56 所示的“配置完成”对话框。如果选择“立即在 Windows 部署服务器上添加映像”复选框，可以在完成 Windows 部署服务的启动后立即启动添加映像向导，这里清除该复选框。

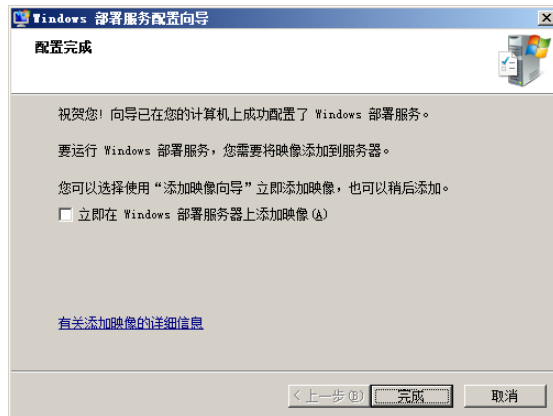


图 14-56 “配置完成” 对话框

⑦ 单击“完成”按钮，完成设置。Windows 部署服务已经可以为企业提供 Windows 系统的部署服务，“Windows 部署服务”窗口如图 14-57 所示。

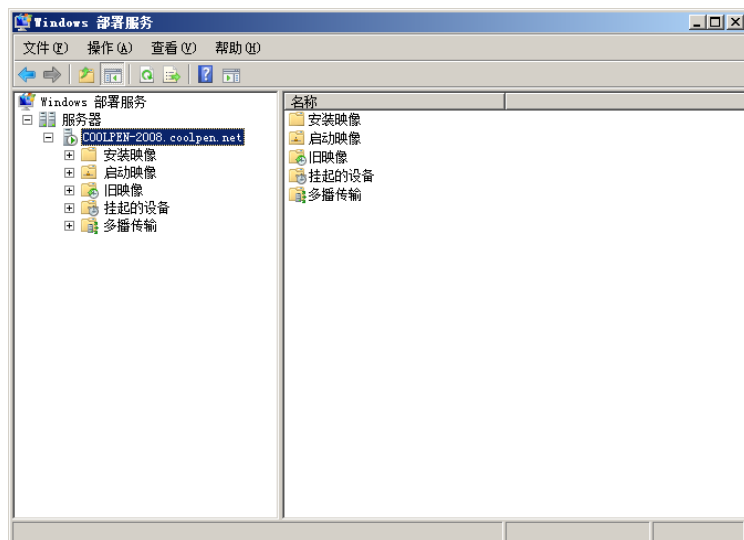


图 14-57 “Windows 部署服务” 窗口

第 15 章 配置与管理 系统更新服务

Windows 系统虽然以操作简单及界面友好的特点赢得了广大用户的青睐，但是层出不穷的漏洞却时时威胁着系统的安全，因此微软公司也会经常发布各种更新和补丁程序。但当网络中计算机数量较多时，同时更新还会占用大量 Internet 带宽。而利用 WSUS (Windows Server Update Services, Windows 服务器更新服务)，可从微软网站下载所有的 Windows 更新，供局域网中的客户端下载安装。从而提高下载速度，并且节省大量 Internet 带宽。

15.1 WSUS 3.0 概述与系统需求

WSUS 是微软推出的网络化补丁分发方案，用其可以集中下载所有的微软产品更新。使客户端可以从 WSUS 服务器快速并方便地下载所需要的更新，而不必连接到微软网站下载，从而节省带宽并提高效率。

15.1.1 WSUS 概述

由于微软的操作系统与应用软件拥有庞大的用户群，因此被发现的“漏洞”也非常多。继而引发诸多的安全问题，解决该问题的唯一办法就是为系统和软件打补丁。借助 WSUS，在企业内部网络中部署升级服务器可以为网络中所有的服务器或者工作站自动更新补丁，降低安全性风险。

WSUS 的当前最新版本为 WSUS 3.0 SP1，其中增加了对 Windows Vista 和 Windows Server 2008 的支持。它不但可以更新更多的 Windows 补丁，同时具有报告功能和导入导出性能，网络管理员还可以控制更新过程。相对早期版本的 WSUS，无论从管理方式、升级速度，以及对磁盘空间的占用率都有了很大的改进。使用 WSUS 3.0 可以对网络中的计算机进行统计和分析，了解已经安装补丁和需要安装的情况。

WSUS 3.0 支持微软公司全部产品的更新，不仅支持微软操作系统，例如 Windows 2000、Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008，还提供了对 Office、SQL Server、MSDE 和 Exchange Server 等内容的更新支持。通过 WSUS 这个内部网络中的 Windows 升级服务，所有的 Windows 更新都集中下载到内部网的 WSUS 服务器中，而网络中的客户端则通过该服务器来得到更新。

15.1.2 WSUS 3.0 系统需求

WSUS 3.0 SP1 对操作系统的要求如下。

(1) 服务器必须运行 Windows Server 2003 SP1 或 Windows Server 2008 操作系统，Windows 2000 系统不支持 WSUS 3.0 SP1。

(2) 服务器最好不要安装终端服务，以免造成安装失败。

在 WSUS 服务器中必须安装如下组件。

(1) IIS，但不要在 IIS 5.0 隔离模式下运行。

(2) MMC 3.0。

(3) Microsoft .NET Framework 2.0 版。

(4) Microsoft Report Viewer 2005 SP1。

15.1.3 文件系统需求

WSUS 3.0 SP1 对服务器文件系统的需求如下。

- (1) 服务器分区使用 NTFS 文件系统。
- (2) 系统分区中有 1 GB 的磁盘可用空间。
- (3) 存储数据库文件的卷中有 2 GB 的磁盘可用空间。
- (4) 存储内容的卷中有 20 GB 的磁盘可用空间。
- (5) 不能在压缩驱动器中安装 WSUS 3.0 SP1。

15.1.4 WSUS 的体系结构

通常情况下，Windows 操作系统从 Microsoft Update 站点或者其他合作站点下载微软产品的补丁（如图 15-1 所示）。然后手动安装，家庭或者中小企业用户大多使用这种方式。但是如果网络规模较大，计算机数量较多，那么就会占用大量的网络带宽，从而影响其他网络应用。另外，Windows 补丁并不是一起发布的，可能每隔一段时间发布几次补丁。如果手动下载更新，就会占用系统管理员和用户的很多时间。

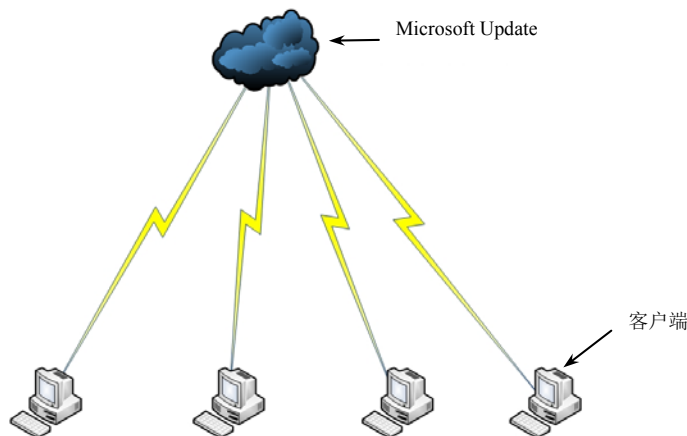


图 15-1 普通用户升级方式

WSUS 是企业内部的升级服务器，它可以从 Microsoft Update 站点下载所有的 Microsoft 更新，而客户端则从 WSUS 服务器升级（如图 15-2 所示）。这样不仅大大减少了带宽的占用，并且可以管理客户端使其“自动”升级。

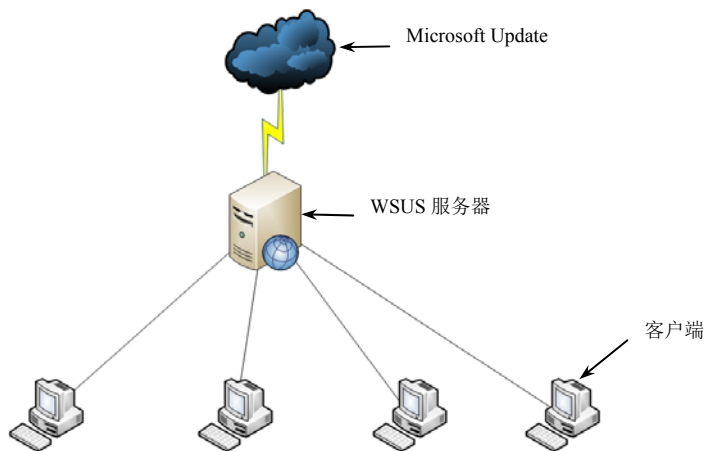


图 15-2 WSUS 体系结构

如果企业网络规模比较大,采用一台 WSUS 服务器不能满足需要,可以采用“多级”WSUS 的体系结构。即为不同网络配置“下游”WSUS 服务器,从“上游”WSUS 服务器下载更新。而“上游”WSUS 服务器直接从 Microsoft Update 站点下载更新,如图 15-3 所示。

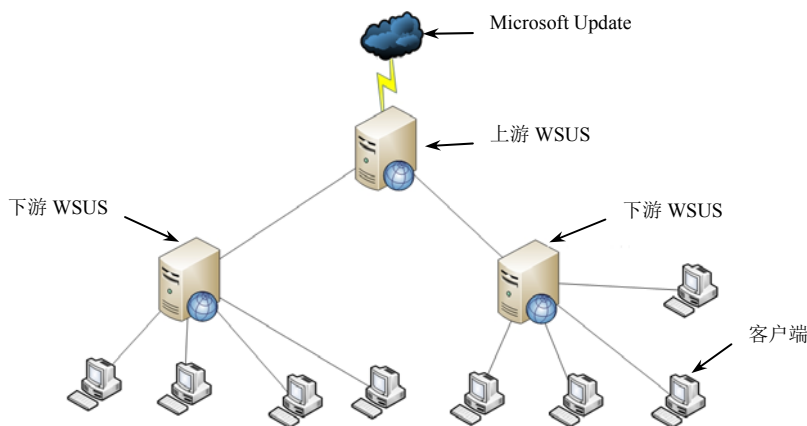


图 15-3 多级 WSUS 体系结构

15.1.5 客户端自动更新要求

WSUS 对客户端操作系统的要求如下。

- (1) Windows Vista 或更高版本。
- (2) Windows Server 2008 或更高版本。
- (3) Windows Server 2003, 任意版本。
- (4) Windows XP Professional SP2 或更高版本。
- (5) Windows 2000 SP4。

15.2 安装与配置 WSUS 3.0

WSUS 并不是 Windows Server 2003/2008 自带的服务,需要从微软网站下载安装专门的安装程序。安装完成后会自动启动配置向导,可用来完成一系列的配置。当然,在安装之前还需要做好准备工作。

15.2.1 全新安装 WSUS 3.0 服务器的准备

在即将安装 WSUS 的计算机中安装 Windows Server 2008 系统,配置网卡的 IP 地址信息,使之能够连接到 Internet。安装 WSUS 之前应做好如下准备工作。

- (1) 安装 IIS 服务。
- (2) 安装后台智能传输服务 (BITS) 2.0。
- (3) 建议安装 Report Viewer。

1. 安装 IIS

在 Windows Server 2008 中安装 IIS 时,必须安装以下组件。

- (1) Windows 身份验证。
- (2) 静态内容。
- (3) ASP.NET。
- (4) IIS 6 管理兼容性。
- (5) IIS 6 元数据库兼容性。

安装步骤如下。

① 在 Windows Server 2008 服务器中运行“添加角色向导”。在如图 15-4 所示的“选择服务器角色”对话框中选中“Web 服务器 (IIS)”复选框。

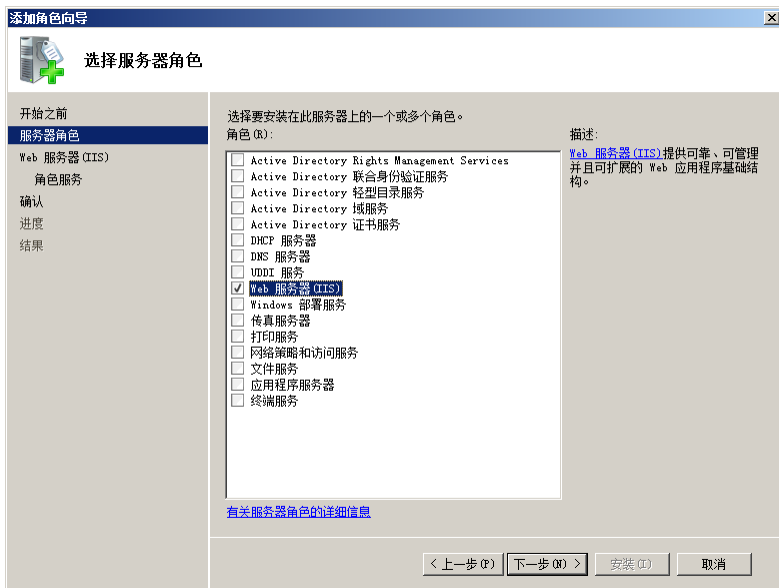


图 15-4 “选择服务器角色”对话框

② 在如图 15-5 所示的“选择角色服务”对话框中为了能够顺利安装 WSUS，可选中除“FTP 发布服务”之外的所有复选框。单击“下一步”按钮安装即可。

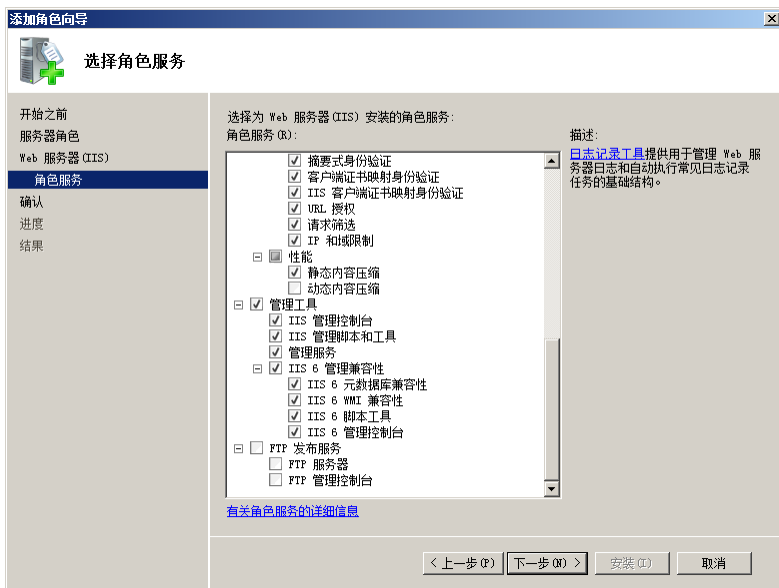


图 15-5 “选择角色服务”对话框

2. 安装 BITS

IIS 组件安装完成后，在“服务器管理器”窗口中单击“添加功能”链接。启动“添加功能向导”，在如图 15-6 所示的“选择功能”对话框中选择安装“BITS 服务器扩展”复选框。由于 Windows Server 2008 系统默认已经集成 Microsoft .NET Framework 组件，所以此处不必选择。



图 15-6 “选择功能”对话框

提示

在 Windows Server 2003 SP1 或 R2 系统中，可通过“Windows 组件向导”来安装 IIS、BITS 和 Microsoft .NET Framework 组件，如图 15-7 所示。如果 Windows Server 2003 没有安装 SP1 或 R2，则默认不提供 Microsoft .NET Framework 组件，可通过如下超级链接获取 .NET Framework 2.0 的安装程序：

<http://www.microsoft.com/downloads/details.aspx?familyid=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=zh-cn>



图 15-7 安装所需服务组件

提示

WSUS 的顺畅运行不仅需要这些服务组件的支持，还取决于 WSUS 客户端的数量。通常情况下，拥有 500 个客户端的 WSUS 服务器 CPU 主频应高于 1 GHz，内存应大于 1 GB。

3. 安装 Report Viewer

Microsoft Report Viewer 是使用 WSUS 3.0 SP1 用户界面的必备组件，可以查看 WSUS 更新或同步的各种报告。如果没有安装该组件，则安装 WSUS 时将显示如图 15-8 所示的“使用管理 UI 所需的组件”对话框，并且不能查看报告。

Microsoft Report Viewer Redistributable 2005 SP1 的下载地址为：

<http://www.microsoft.com/downloads/details.aspx?familyid=E7D661BA-DC95-4EB3-8916-3E31340DDC2C&displaylang=zh-cn>

安装步骤如下。

- ① 运行 Report Viewer 安装程序，启动报表安装向导，如图 15-9 所示。



图 15-8 “使用管理 UI 所需的组件”对话框



图 15-9 报表安装向导

- ② 单击“下一步”按钮，显示如图 15-10 所示的“最终用户许可协议”对话框，选中“我已阅读并接受许可条款”复选框。

- ③ 单击“安装”按钮开始安装，完成后显示如图 15-11 所示的“安装完成”对话框。

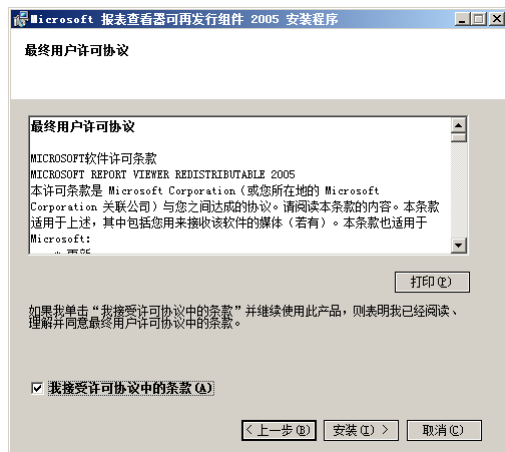


图 15-10 “最终用户许可协议”对话框



图 15-11 “安装完成”对话框

- ④ 单击“完成”按钮。

15.2.2 安装 WSUS 服务器

WSUS 3.0 SP1 安装程序可以从如下站点下载：

<http://www.microsoft.com/downloads/details.aspx?FamilyId=F87B4C5E-4161-48AF-9FF8-A96993C688DF&displaylang=en>

WSUS 的安装过程如下。

- ① 运行 WSUS 3.0 SP1 安装程序，启动 WSUS 安装向导，如图 15-12 所示。
- ② 单击“下一步”按钮，显示如图 15-13 所示的“安装模式选择”对话框。选择默认的“包括管理控制台的完整服务器安装”单选按钮；选择“仅限管理控制台”单选按钮，只安装 WSUS 服务器管理控制台工具，可用来管理远程 WSUS 服务器。

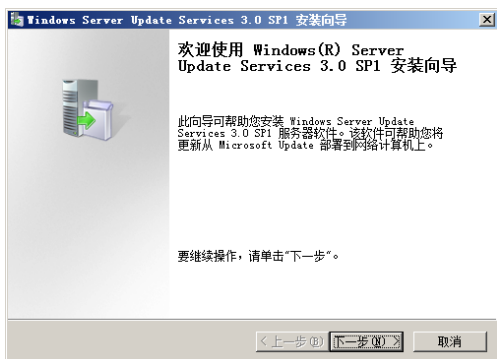


图 15-12 WSUS 安装向导

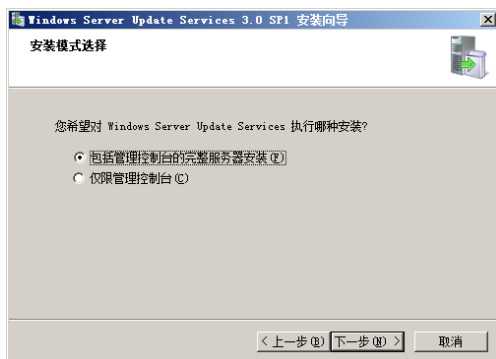


图 15-13 “安装模式选择”对话框

③ 单击“下一步”按钮，显示如图 15-14 所示的“许可协议”对话框。选择“我接受许可协议条款”单选按钮，同意许可协议。

④ 单击“下一步”按钮，显示如图 15-15 所示的“选择更新源”对话框。选中“本地存储更新”复选框，指定存储更新文件的位置。为了系统安全，应选择空间较大的非系统分区。



图 15-14 “许可协议”对话框



图 15-15 “选择更新源”对话框

⑤ 单击“下一步”按钮，显示如图 15-16 所示的“数据库选项”对话框。选择“在此计算机上安装 Windows Internal Database”单选按钮，并指定保存 WSUS 数据库文件的位置。WSUS 数据库中存储的信息包括 WSUS 服务器配置信息、用于描述更新程序作用的元数据和客户端、更新程序信息，以及客户端所进行的更新情况，通常不会占用太多空间。



图 15-16 “数据库选项”对话框



提示

WSUS 还可以使用本地或远程计算机上的 SQL Server 2000/2005 数据库，但需要注意的是 WSUS 只支持 Windows 认证。如果是独立的 WSUS 服务器，则建议使用其默认的数据库。

⑥ 单击“下一步”按钮，显示如图 15-17 所示的“网站选择”对话框。选择“使用现有 IIS 默认网站”单选按钮，即可使用系统默认的 80 端口作为此站点的通信端口。如果当前服务器上存在正在运行的 Web 站点，且已占用 80 端口，则可以选择“创建 Windows Server Update Services 3.0 SP1 网站”单选按钮，使用 8530 端口创建用于 WSUS 管理的 Web 站点。

⑦ 单击“下一步”按钮，显示如图 15-18 所示的“准备安装 Windows Server Update Services 3.0 SP1”对话框。其中显示当前设置的安装信息，单击“上一步”按钮可返回重新修改。



图 15-17 “网站选择”对话框



图 15-18 “准备安装 Windows Server Update Services 3.0 SP1”对话框

⑧ 单击“下一步”按钮，开始安装 WSUS。完成后显示如图 15-19 所示的“正在完成 Windows Server Update Services 3.0 SP1 安装向导”对话框，提示已成功安装。

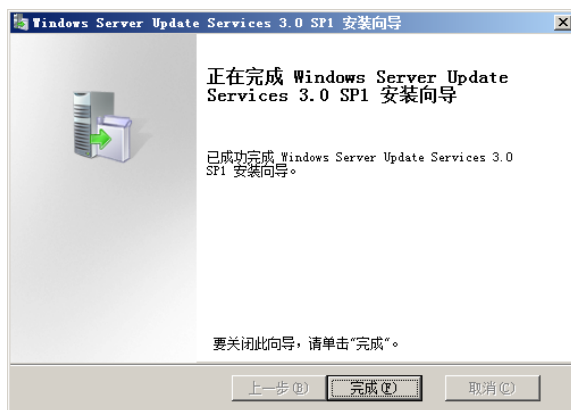


图 15-19 “正在完成 Windows Server Update Services 3.0 SP1 安装向导”对话框

⑨ 单击“完成”按钮，关闭 WSUS 安装向导。系统会自动启动 WSUS 配置向导，用来配置 WSUS 服务器的相关选项。

15.2.3 WSUS 3.0 配置向导

WSUS 安装完成以后，默认自动启动配置向导以完成详细的配置工作。即使取消配置向导，重新打开 WSUS 时也会自动启动配置向导。操作步骤如下。

① WSUS 3.0 SP1 安装完成后自动打开如图 15-20 所示的“Windows Server Update Services 配置向导”对话框，其中显示需要执行的准备工作，用户也可以通过单击“开始”→“管理工具”→“Microsoft Windows Server Update Services 3.0 SP1”选项来启动该向导。

② 单击“下一步”按钮，显示如图 15-21 所示的“加入 Microsoft Update 改善计划”对话框，根据需要选择是否加入 Microsoft Update 改善计划。

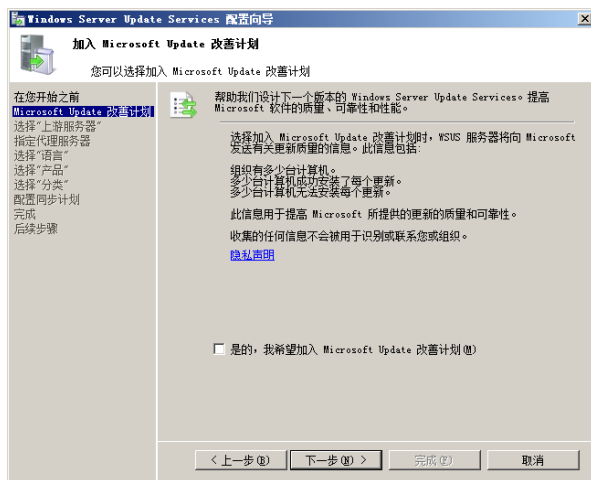
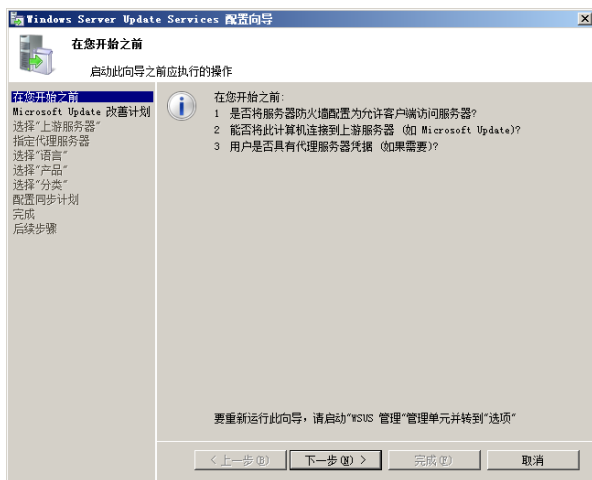


图 15-20 “Windows Server Update Services 配置向导”对话框 图 15-21 “加入 Microsoft Update 改善计划”对话框

③ 单击“下一步”按钮，显示如图 15-22 所示的“选择‘上游服务器’”对话框。系统默认选择“从 Microsoft Update 进行同步”单选按钮，即直接从微软更新服务器获取更新。

提示 如果网络中已部署有 WSUS 服务器，则选择“从其他 Windows Server Update Services 服务器进行同步”单选按钮并在“服务器名”文本框中输入上游 WSUS 服务器的 IP 地址或计算机名，如图 15-23 所示，这样可以较快地获得更新。

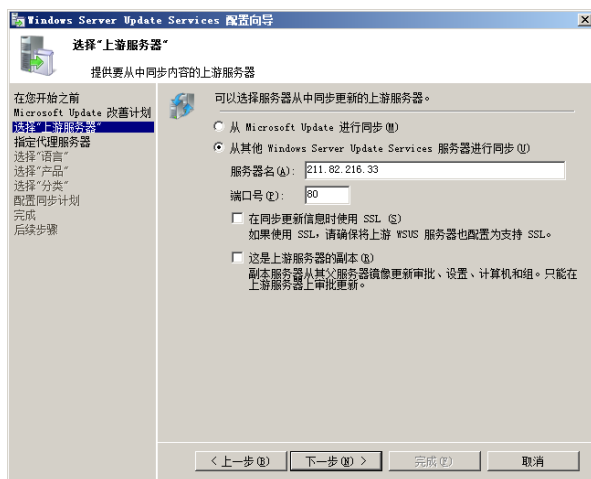
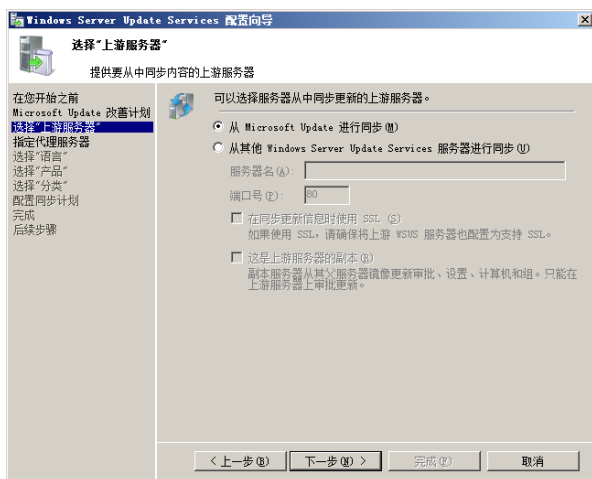


图 15-22 “选择‘上游服务器’”对话框

图 15-23 输入上游 WSUS 服务器的 IP 地址或计算机名

④ 单击“下一步”按钮，显示如图 15-24 所示的“指定代理服务器”对话框，设置当前 WSUS 服务器访问 Internet 的方式。如果网络中没有设置代理服务，则不必设置。

⑤ 单击“下一步”按钮，显示如图 15-25 所示的“连接到上游服务器”对话框。单击“开始连接”按钮，当前 WSUS 服务器将从 Microsoft Update 或者其上游服务器获得更新信息。其中包括可用更新类型、可以更新的产品和可用语言，并且测试连接是否正常。

⑥ 连接成功后单击“下一步”按钮，显示如图 15-26 所示的“选择‘语言’”对话框。选择“仅下载这些语言的更新”单选按钮，并在列表框中选择需要的语言类型。如果选择“下载包括新语言在内的所有语言的更新”单选按钮，将下载所有语言类型的更新，适用于含有多种语言版本的网络。



图 15-24 “指定代理服务器”对话框



图 15-25 “连接到上游服务器”对话框

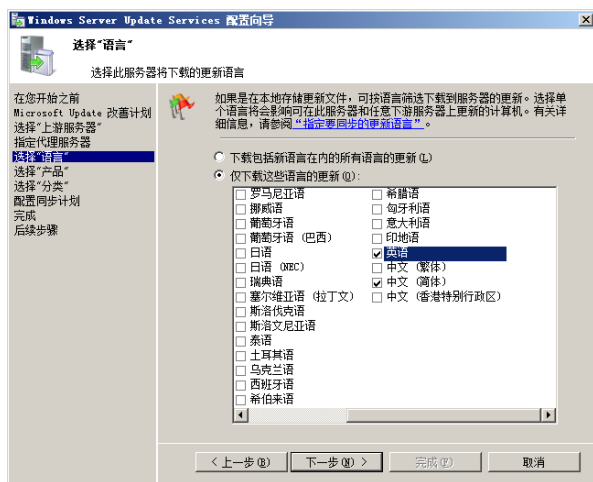


图 15-26 “选择‘语言’”对话框



如果当前 WSUS 服务器是从“上游”WSUS 服务器更新，则显示“下载上游服务器支持的所有语言的更新”或“仅下载这些语言的更新（上游服务器只支持标有星号的语言）”单选按钮。



⑦ 单击“下一步”按钮，显示如图 15-27 所示的“选择‘产品’”对话框，选择当前 WSUS 服务器将要下载更新的产品。在第 1 次同步时，建议选中“所有产品”复选框。使 WSUS 自动搜索所有微软产品，以便日后可以为其他新产品提供更新服务。如果当前 WSUS 服务器选择从“上游”服务器升级，则不会出现此对话框。

⑧ 单击“下一步”按钮，显示如图 15-28 所示的“选择‘分类’”对话框。指定要同步的更新分类，第 1 次使用时建议选择“所有分类”复选框。如果当前 WSUS 服务器选择从“上游”服务器升级，则不会出现此对话框。

⑨ 单击“下一步”按钮，显示如图 15-29 所示的“设置同步计划”对话框，选择当前 WSUS 服务器同步的方式与时间。建议设置为“自动同步”方式，使 WSUS 无需人工参与即可自动完成同步操作。另外，由于同步过程中将占用大量带宽，因此建议选择网络空闲的时间（例如，每天的非工作时间），以避免影响其他网络用户的正常应用。

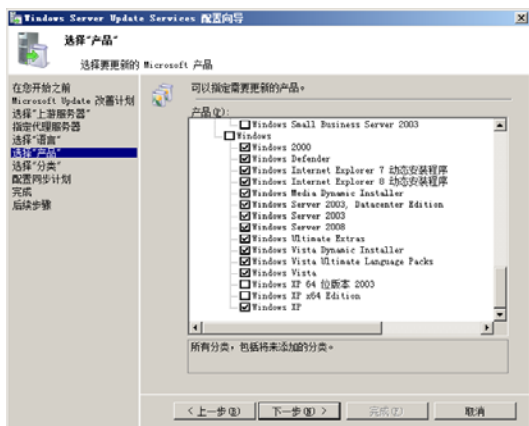


图 15-27 “选择‘产品’”对话框

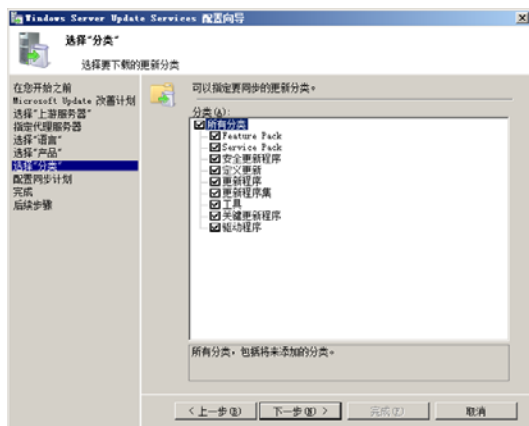


图 15-28 “选择‘分类’”对话框

⑩ 单击“下一步”按钮，显示如图 15-30 所示的“完成”对话框，选中“启动 Windows Server Update Services 管理控制台”和“开始初始同步”复选框。

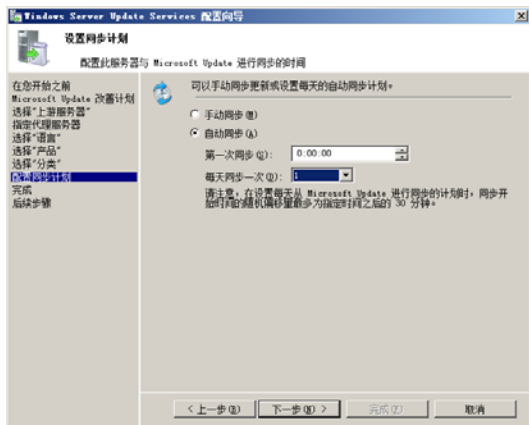


图 15-29 “设置同步计划”对话框

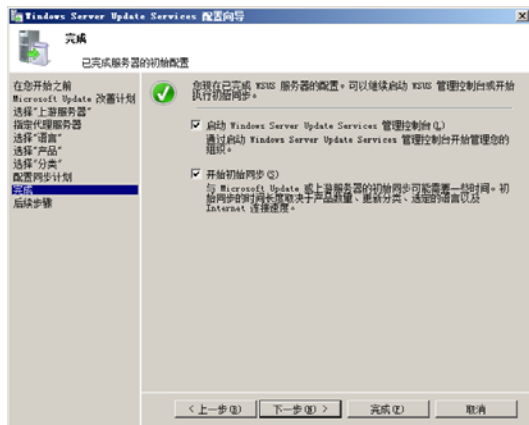


图 15-30 “完成”对话框



提示

如果在此之前运行过该配置向导，则“启动 Windows Server Update Services 管理控制台”复选框不可用。

⑪ 单击“下一步”按钮，显示如图 15-31 所示的“后续步骤”对话框，提示需要用户手动配置的内容。

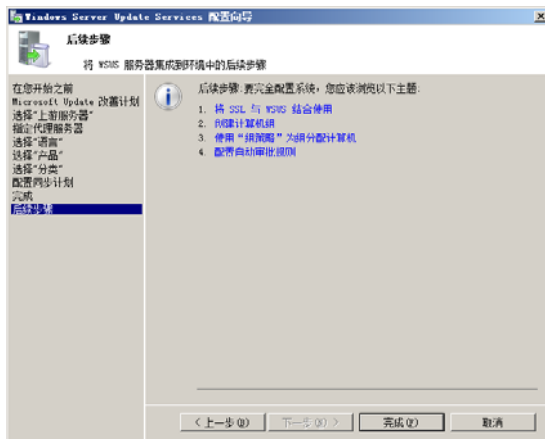


图 15-31 “后续步骤”对话框

- ⑫ 单击“完成”按钮，WSUS 配置完成并自动执行第 1 次同步。

15.3 配置客户端

由于 WSUS 的目的是为 Windows 客户端提供更新，因此任何 Windows 操作系统都可以从 WSUS 服务器下载更新，但需要通过组策略进行配置。早期版本的 Windows 操作系统。需要安装 WSUS 客户端才能从 WSUS 服务器获取更新。需要注意的是，将客户端配置为 WSUS 客户端后，“控制面板”窗口中的自动更新将无法设置。

15.3.1 安装 WSUS 客户端

默认情况下，Windows 9x 和 Windows 2000 SP2 系统由于未安装 SUS 客户端程序，因此无法从 WSUS 服务器获取更新。用户需要下载 WSUS 客户端程序并安装，才能配置为通过 WSUS 服务器获取系统更新。而 Windows 2000 SP2 系统之后的版本均内置了 SUS 客户端程序，可以直接从 WSUS 服务器获取更新。

SUS 客户端程序的下载地址为 <http://nj.onlinedown.net/soft/35844.htm>。

15.3.2 通过本地策略配置客户端

通过组策略或本地策略编辑器配置 WSUS 客户端是最常用的方法之一，如果是在域环境中，系统管理员可以组策略来集中部署；而工作组中的计算机则需要在每台计算机上修改本地策略使其成为 WSUS 客户端。

1. Windows 2000 的设置

① 以管理员身份登录，单击“开始”→“运行”选项。在“运行”对话框中输入 `gpedit.msc` 命令，单击“确定”按钮，打开如图 15-32 所示的“组策略”窗口。

② 展开“计算机配置”→“管理模板”选项，右击“管理模板”选项并选择快捷菜单中的“添加/删除模板”。打开“添加/删除模板”对话框，如图 15-33 所示。

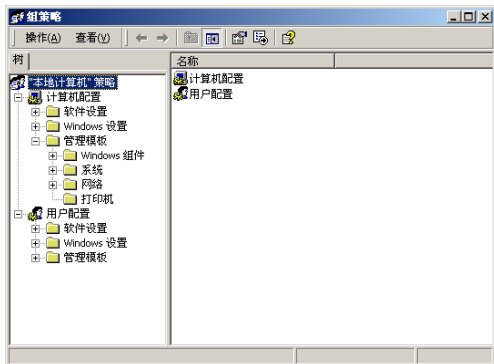


图 15-32 “组策略”窗口

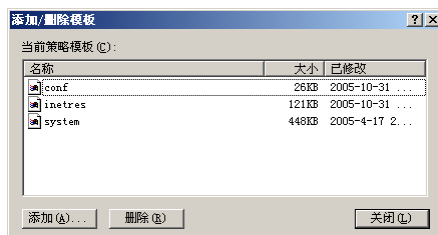


图 15-33 “添加/删除模板”对话框

③ 单击“添加”按钮，在如图 15-34 所示的“策略模板”对话框中选择“wuau.adm”选项。单击“打开”按钮，添加到“添加/删除模板”对话框中。

④ 单击“关闭”按钮，返回“组策略”窗口。展开“管理模板”→“Windows 组件”→“Windows Update”选项，如图 15-35 所示。此时，即可配置从 WSUS 服务器获取更新。

⑤ 双击“配置自动更新”选项，显示如图 15-36 所示的“配置自动更新 属性”对话框。选择“启用”单选按钮，在“配置自动更新”下拉列表框中选择自动更新的方式，建议选择“3 - 提醒下载并提醒安装”选项，单击“确定”按钮即可。

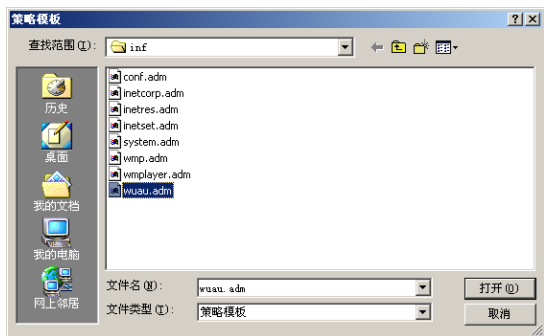
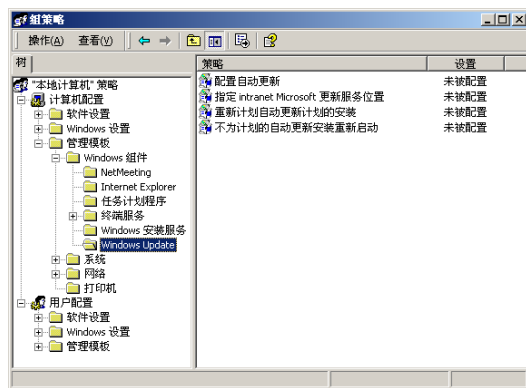


图 15-34 “策略模板”对话框

图 15-35 展开“管理模板”→“Windows 组件”
→“Windows Update”选项

⑥ 在“组策略”窗口中双击“指定 Intranet Microsoft 更新服务器位置”选项，显示如图 15-37 所示的“指定 Intranet Microsoft 更新服务器位置 属性”对话框。选择“启用”单选按钮，在“设置检测更新的 intranet 更新服务”和“设置 intranet 统计服务器”文本框中分别键入 WSUS 服务器地址，格式为“http://WSUS 名称或 IP 地址”。

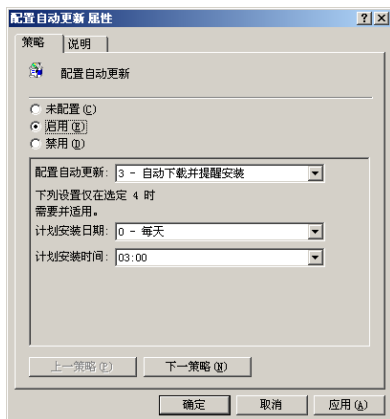


图 15-36 “配置自动更新 属性”对话框

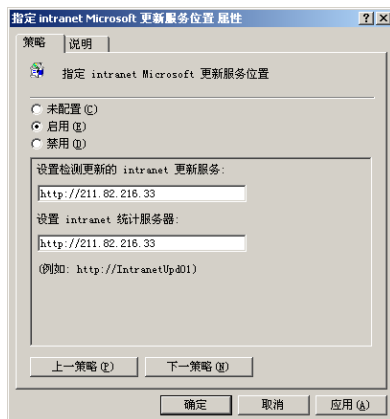


图 15-37 “指定 Intranet Microsoft 更新服务器位置 属性”对话框



提示

如果 WSUS 服务器没有使用默认端口，则指定更新服务器和统计服务器时也需要指定匹配的通信端口，如 http://211.82.216.33:8530。

⑦ 单击“确定”按钮保存设置，这样 Windows 2000 即可自动从 WSUS 服务器获取更新。

2. Windows XP/Vista 的设置

Windows XP/2003/Vista/2008 系统通过组策略配置自动更新的操作步骤相同，这里以 Windows Vista 为例介绍。

① 以管理员账户登录计算机，打开“开始”菜单。在“开始搜索”文本框中输入“gpedit.msc”，按回车键，打开如图 15-38 所示的“策略对象编辑器”窗口，展开“计算机配置”→“管理模板”→“Windows 组件”→“Windows Update”选项。

② 在右侧窗口中双击“配置自动更新”策略，打开如图 15-39 所示的“配置自动更新 属性”对话框。选择“已启用”单选按钮，在“配置自动更新”下拉列表框中选择更新方式。如果选择“自动下载并计划安装”选项，则需要设置“计划安装日期”和“计划安装时间”。完成后单击“确定”按钮，保存设置。

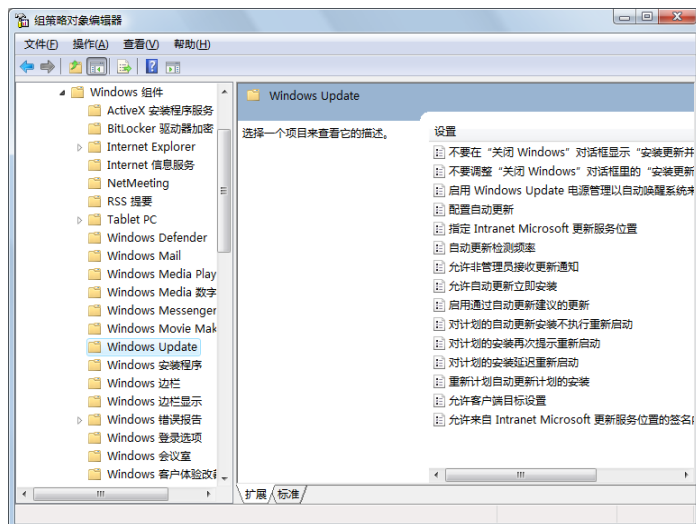


图 15-38 “策略对象编辑器”窗口

③ 在“Windows Update”窗口中双击“指定 Intranet Microsoft 更新服务位置”策略，显示如图 15-40 所示的“指定 Intranet Microsoft 更新服务位置 属性”对话框。在“设置检测更新的 Intranet 更新服务”和“设置 Intranet 统计服务器”文本框中分别输入 WSUS 服务器地址，格式为“http://WSUS 名称或 IP 地址”。

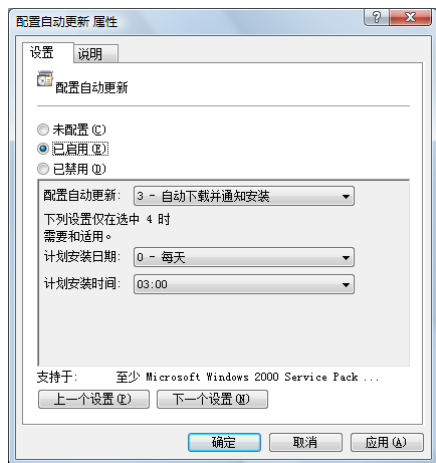


图 15-39 “配置自动更新 属性”对话框

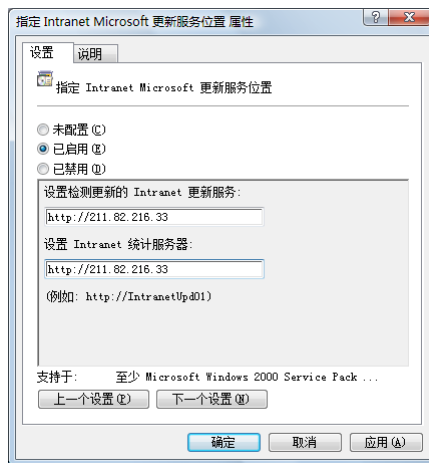


图 15-40 “指定 Intranet Microsoft 更新服务位置 属性”对话框

④ 单击“确定”按钮，系统就会自动从 WSUS 服务器检测并下载更新。单击“开始”→“控制面板”→“Windows Update”选项，显示如图 15-41 所示的“Windows Update”窗口。单击“检查更新”按钮，可以立即检查更新。

提示 可以按照如下方法检查 WSUS 客户端是否生效：配置 WSUS 客户端后，在 Windows 目录下会生成 windowsupdate.log 文件，打开后可以看到此客户端是从何处升级的补丁及升级了哪些补丁。

15.4 配置 WSUS 服务器

WSUS 安装完成以后，还需要经过一系列的配置，包括接入 Internet 方式、获取更新方式、支持的产品分类、同步方式及时间等，使 WSUS 根据网络中所安装的系统及软件下载所需要的更新。

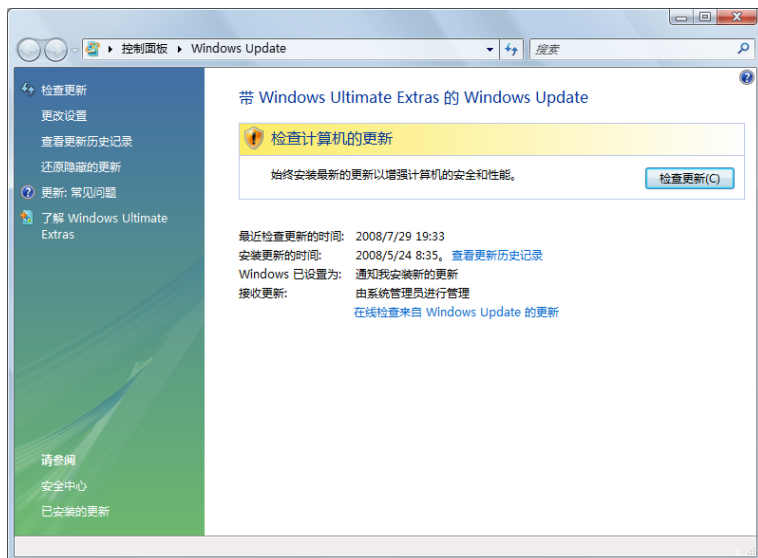


图 15-41 “Windows Update”窗口

15.4.1 WSUS 的更新设置

WSUS 服务器的主要功能就是将所需的更新文件发送至客户端，只有合理有效地管理好这些更新才能快速地为客户端提供服务。更新管理主要包括更新内容和更新操作的管理两部分。

1. 更新内容

更新内容即 WSUS 服务器分发到客户端的安装程序，主要包括元数据和更新文件两部分。在大多数用户看来二者好像是一个文件，客户端需要时候从服务器端下载即可。其实并非如此，Microsoft Update 中的每个可用更新都由以下两个组件构成。

(1) 元数据：主要指更新程序的属性信息及 EULAs (End-User License Agreements 终端用户协议)等相关数据，保存在 WSUS 服务器使用的数据库中。它与安装 WSUS 服务器时的相关设置无关，只能完全下载并保存在指定的数据库中，下载的更新元数据软件包通常远远小于实际的更新文件软件包。

(2) 更新文件：是客户端安装更新时使用的安装包，相对于元数据而言，占用空间较多，通常保存在 WSUS 服务器指定的目录分区中。如果安装 WSUS 服务器时设置的是只下载安装信息而不下载安装文件，则这些文件会保存在微软的 Microsoft Update 站点上。

2. 更新操作

更新操作是 WSUS 服务器应用的重点，主要包括更新的批准、测试及存储管理等。在 WSUS 服务器中，所获得的更新文件只有经过管理审批后才能安装到指定的 WSUS 客户端上。

(1) 分类查看更新

无论更新文件是否保存在本地 WSUS 服务器上，同步之后都可以在 WSUS 控制台上查看到获取的所有的更新文件信息，并且已经分类显示。

在 WSUS 控制台中选择左侧树形目录中的“更新”选项，即可查看所有的更新。包括所有更新、关键更新、安全更新和 WSUS 更新，如图 15-42 所示。同时，分别显示每一类更新中包含更新文件的数量，以及所有客户端中需要该更新的数量等。

选择一个更新分类即可查看所包含的更新内容。例如，选择“关键更新”，在“状态”下拉列表框中选择“任何”选项。单击“刷新”按钮，即可显示所有的关键更新，如图 15-43 所示。可以通过选择不同的“审批”和“状态”，筛选待查看的更新。

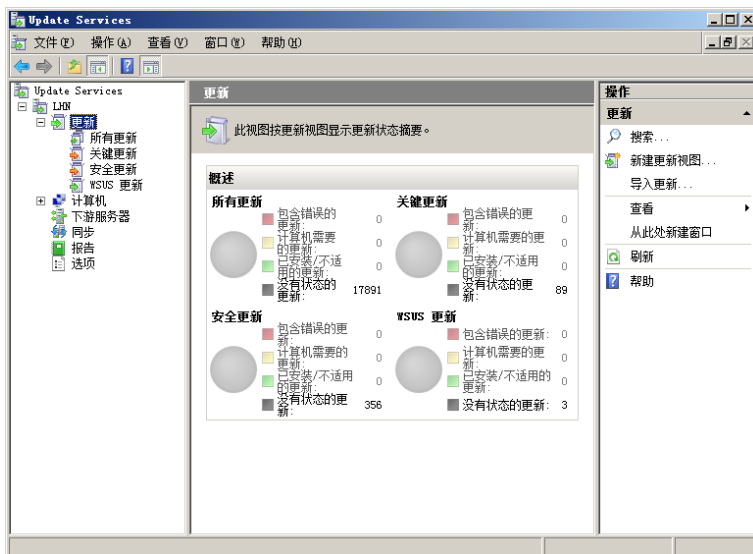


图 15-42 所有的更新



图 15-43 所有的关键更新

(2) 审批更新

审批指系统管理员允许或拒绝将更新程序分发到客户端计算机。为安全起见，系统管理员应查看更新，以决定允许或拒绝安装。对于不适用于指定客户端的更新，可以选择拒绝审批或删除。

在更新程序详细信息窗口中（以“关键更新”为例），右击待审批的更新。选择快捷菜单中的“审批”选项，显示如图 15-44 所示的“审批更新”对话框。单击待审批的计算机组左侧的箭头，在显示的下拉菜单中可以选择审批方式。选择“已审批进行安装”选项，即表示同意将更新安装到该组中的所有计算机。

经过审批的计算机分组会由原来的灰色变为绿色，同时在“审批”列中显示为“安装”，如图 15-45 所示。

审批完成后单击“确定”按钮，显示如图 15-46 所示的“审批进度”对话框。根据审批更新数量的不同，所需时间也会有所不同。审批成功后，在“结果”列表框中显示为“成功”；如果出现错误，则审批结果显示为“失败”。

单击“关闭”按钮，关闭“审批进度”对话框，返回“Update Services”窗口。

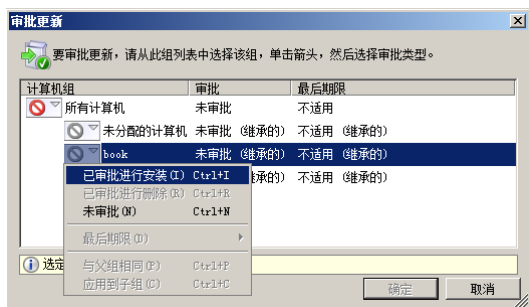


图 15-44 “审批更新”对话框

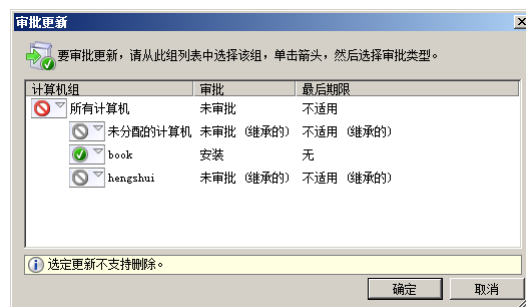


图 15-45 已审批的分组

(3) 拒绝更新

如果某个更新不再使用，则可以在 WSUS 服务器的更新管理窗口中将其拒绝。在拒绝更新时，默认情况下，“更新”窗口中将不再显示并且无法对其进行审批，但可在所有的更新中查看被拒绝的更新。右击要拒绝的更新，并选择快捷菜单中的“拒绝”选项，显示如图 15-47 所示的“拒绝更新”对话框。

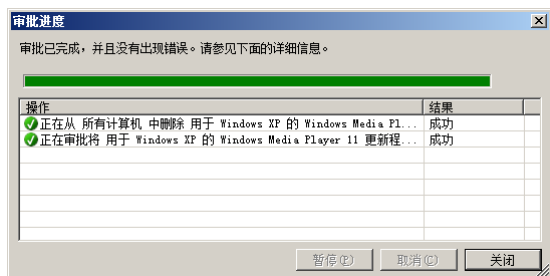


图 15-46 “审批进度”对话框

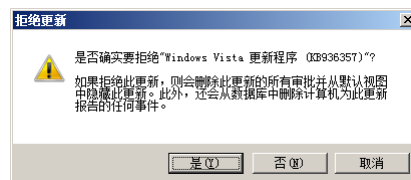


图 15-47 “拒绝更新”对话框

单击“是”按钮，即可拒绝该更新。单击工具栏中的“刷新”按钮，即可发现该更新程序的“审批”状态已变为“已拒绝”，如图 15-48 所示。

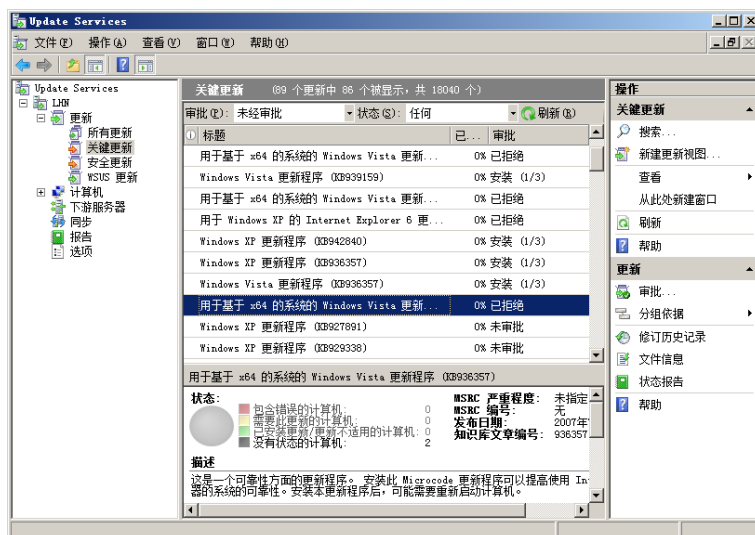


图 15-48 被拒绝的更新

3. WSUS 的备份和恢复

如果在安装和配置 WSUS 服务器时设置了在本地保存更新文件，则可能会需要较大的磁盘空间，并且需要经常整理这些更新。如果要增加硬盘，或者存储更新文件的磁盘或分区出现故障时。更改更新文件的存储路径，此时需要导出 WSUS 服务器中的数据并导入到新磁盘中。WSUS 提供了一个非常

实用的命令行管理工具——WSUSUtil，默认路径是 C:\Program Files\Update Services\Tools>，可以实现 WSUS 导入导出及服务器的迁移等。

打开命令提示符窗口，进入 WSUSUtil 所在目录。运行 WSUSUtil 命令，显示如图 15-49 所示的帮助信息。其中 healthmonitoring、export、import 及 movecontent 等都是 WSUSUtil 的参数，运行带参数的命令，可以继续查看附带该参数后的用法及效果。

Wsusutil 命令常用的参数主要是 export（导出备份）、import（导入备份）和 movecontent（移动目录）。

(1) 导出数据

WSUS 服务器同步后，执行如下命令可以创建更新数据包和日志：

```
wsusutil export d:\wsus.cab d:\test.log
```

按回车键，开始导出更新数据，如图 15-50 所示。导出所需的时间主要取决于 WSUS 服务器存储的更新内容的多少。

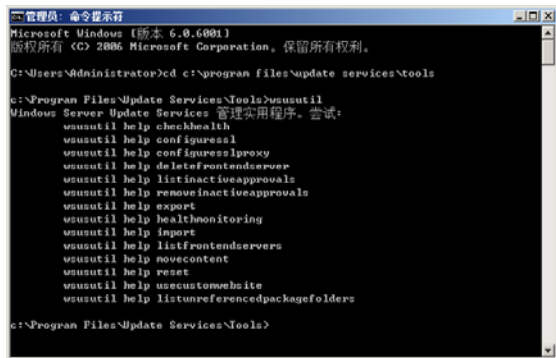


图 15-49 WSUSUtil 帮助信息

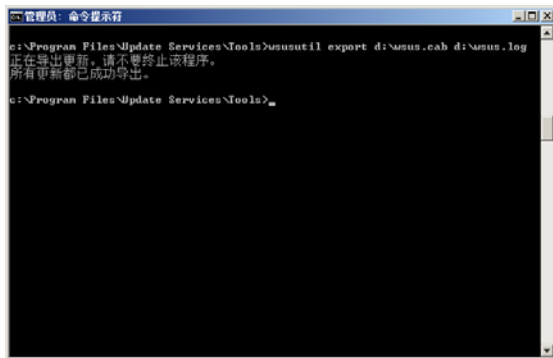


图 15-50 成功导出更新元数据

(2) 导入数据

如果要已备份的数据导入 WSUS 服务器中，则执行如下命令：

```
wsusutil import f:\wsus.cab f:\wsus.log
```

按回车键，开始将数据导入 WSUS 服务器，如图 15-51 所示。

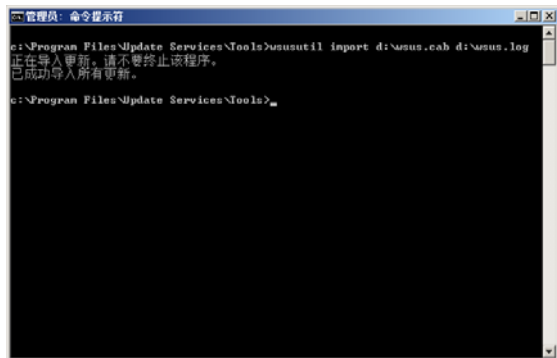


图 15-51 导入备份



注意：

在导入导出备份的过程中千万不可终止操作，否则可能会前功尽弃。

15.4.2 WSUS 服务器中的计算机分组

当 WSUS 安装完成，并且将客户端配置为从 WSUS 服务器获取更新时 WSUS 服务器就会发现这

些计算机，并显示在 WSUS 控制台中。为了便于管理，WSUS 可以根据操作系统或者所属性的部门分组客户端，而未分组的 WSUS 客户端都将存储在“未分配的计算机”分组中。

1. 查看计算机

(1) 在“Update Services”窗口中选择“计算机”选项，显示的“计算机”窗口如图 15-52 所示，其中显示连接到 WSUS 服务器的计算机摘要信息。

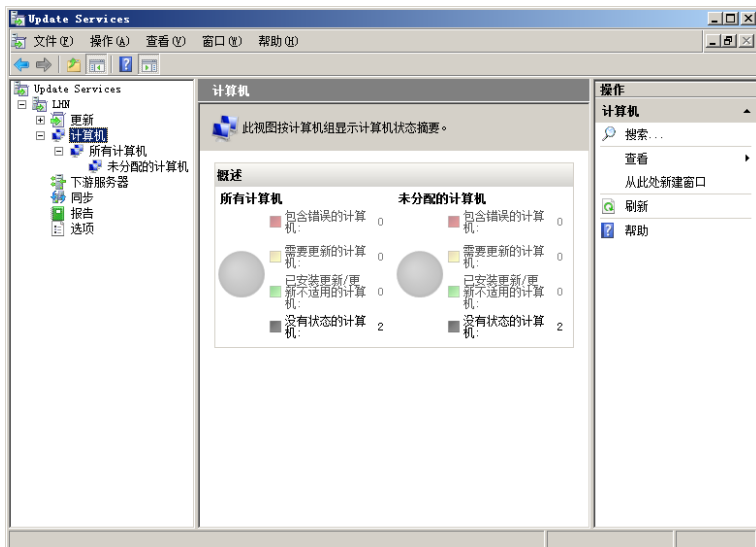


图 15-52 “计算机”窗口

(2) 选择“所有计算机”选项，显示所有客户端的状态，如图 15-53 所示。在“状态”下拉列表框中可以选择显示哪种状态的计算机，例如“任何”选项。单击“刷新”按钮，显示所有的客户端。而在下方的“状态”下拉列表框中显示计算机的详细信息，包括操作系统版本、IP 地址甚至计算机型号、处理器及 BIOS 版本等信息。

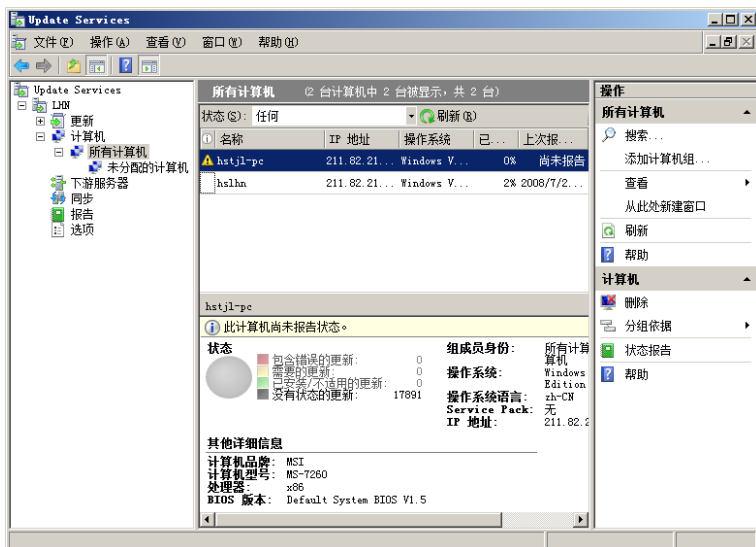


图 15-53 所有客户端的状态

2. 管理计算机分组

为了便于管理客户端，可以分组计算机，将不同操作系统的计算机添加到不同的组中。

(1) 选择“所有计算机”选项，右击并选择快捷菜单中的“添加计算机组”选项。显示如图 15-54 所示的“添加计算机组”对话框，在“名称”文本框中输入计算机组的名称。



图 15-54 “添加计算机组”对话框

(2) 单击“添加”按钮，添加完成一个计算机组，如图 15-55 所示。按照同样步骤，可添加多个计算机组。



图 15-55 添加成功的计算机组

(3) 在“所有计算机”或者“未分配的计算机”窗口中，选择要添加到组的计算机。右击并选择快捷菜单中的“更改成员身份”选项，显示如图 15-56 所示的“设置计算机组成员身份”对话框，选中要添加到的组的复选框即可。

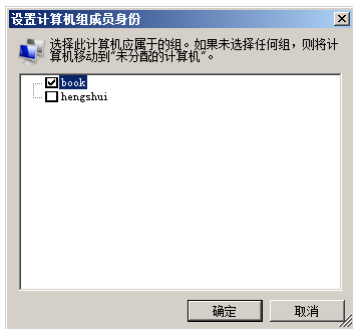


图 15-56 “设置计算机组成员身份”对话框

(4) 单击“确定”按钮，将该计算机添加到相应的组中，如图 15-57 所示。如果要更改计算机所属的组，也可按照同样步骤操作。

3. 删除组或计算机

如果需要删除计算机分组，可右击分组名称，选择快捷菜单中的“删除”选项。如果当前组中没有计算机，就会被直接删除；如果该组中包含有计算机，则会显示如图 15-58 所示的“删除计算机组”对话框，可选择以下选项。

(1) 从此组中删除计算机：只从该组中删除计算机，但不会影响计算机在其他分组中的存在和应用。



图 15-57 添加到组中的计算机

(2) 将计算机移到此组的父组中：将组中的计算机移动到父组中。由于该组的父组是“所有计算机”，默认已经存在该计算机，所以不可操作。

(3) 从此 WSUS 服务器中删除计算机：彻底删除本组的计算机，如果其他分组中也有该计算机，则一并删除。

选择一个选项后单击“删除”按钮，该组即可从 WSUS 中删除。

如果某个客户端不再需要从 WSUS 服务器获取更新，或者由于其他原因退出网络时，应及时从 WSUS 服务器中删除。选择要删除的计算机名称。右击并选择快捷菜单中的“删除”选项，显示如图 15-59 所示的“删除计算机”对话框，单击“是”按钮即可将其从 WSUS 服务器中删除。

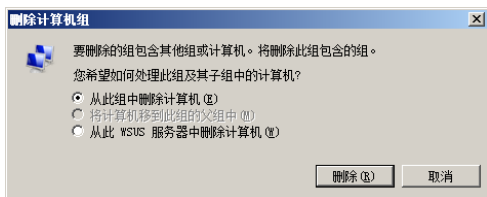


图 15-58 “删除计算机分组”对话框

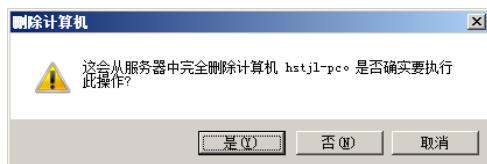


图 15-59 “删除计算机”对话框

15.4.3 同步

“同步”即当前 WSUS 服务器从 Microsoft Update 站点或其上游 WSUS 服务器获取更新的过程，同步可以使用手动同步和自动同步两种方式。应根据网络的使用情况来决定何时同步，通常应将同步计划设置为访问 Internet 较少的时间段，例如凌晨。如果网络带宽资源紧张，则可使用手动同步方式。

(1) 在 WSUS 控制台窗口中选择“同步”选项，显示如图 15-60 所示的“同步”窗口。其中列出最近完成的同步信息，单击一个同步信息，在下面的“同步详细信息”下拉列表框中显示该次同步的启动时间、完成时间、结果及类型等。

(2) 单击“操作”列表框中的“立即同步”链接开始同步，如图 15-61 所示。在“同步状态”列表框中显示当前的同步状态及进度，但不显示本次同步的时间、类型及结果等信息。

15.4.4 报告

WSUS 服务器提供了报告监视功能，可以实时监控 WSUS 服务器的运行情况和客户端安全状态，包括更新报告、计算机报告和同步报告 3 类，如图 15-62 所示。需要注意的是，必须在 WSUS 服务器中安装 Microsoft Report Viewer Redistributable 2005 SP1；否则无法查看报告内容。默认情况下，WSUS

Reporters 安全组的成员及本地 Administrator 具有运行和查看 WSUS 报告的权限。

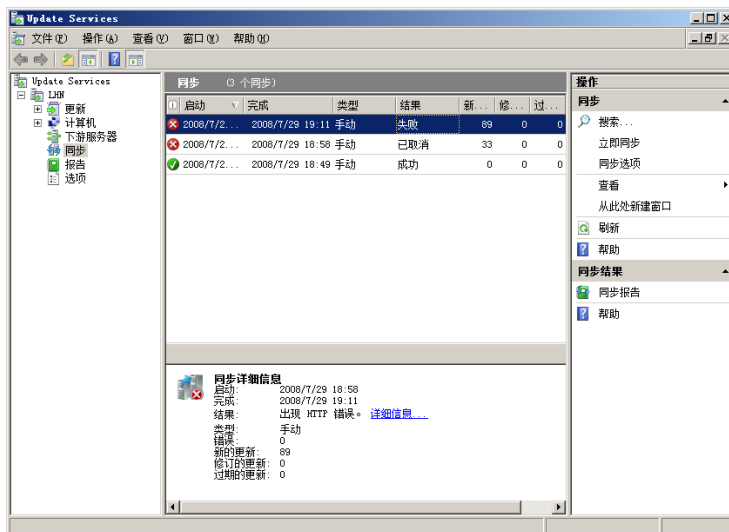


图 15-60 “同步”窗口

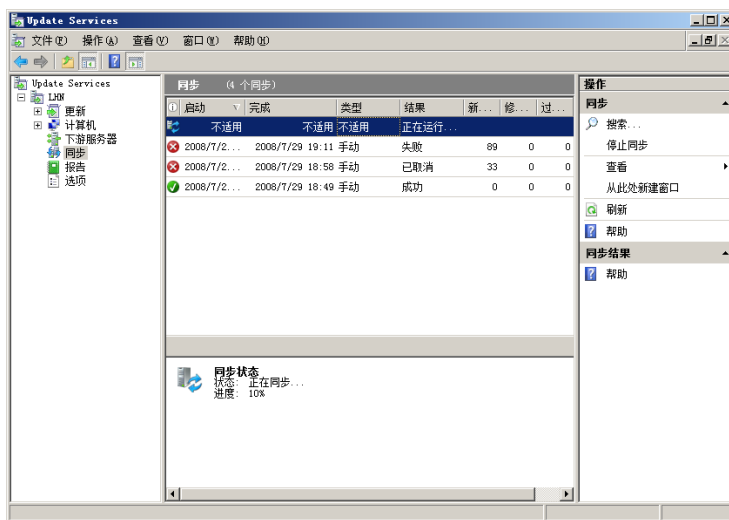


图 15-61 开始同步

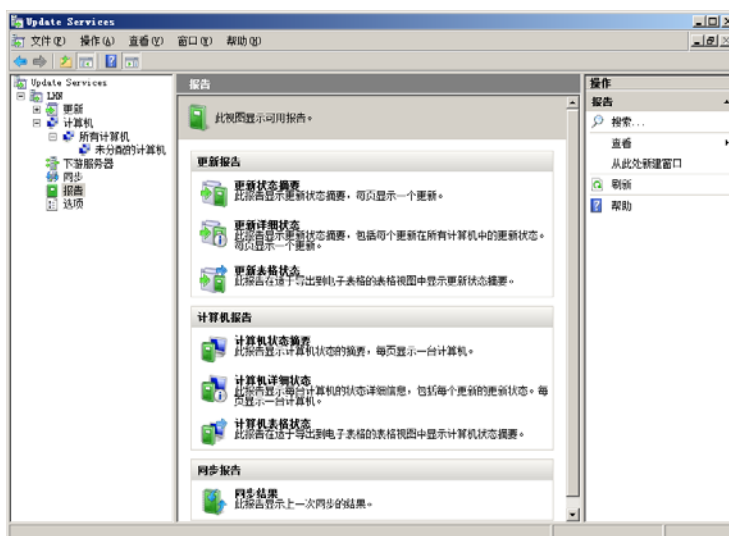


图 15-62 3 类报告

1. 更新报告

更新报告共包括如下 3 种。

- (1) 更新状态摘要报告：提供每个更新的详细摘要，包括更新属性和审批状态。生成此报告时，将会显示报告条件中包含的所有更新。
- (2) 更新状态详细报告：显示所有计算机中各个更新的状态。
- (3) 更新状态表格报告：提供多个更新的更新状态。生成此报告时，将会在表中看到报告条件中包含的所有更新。

查看各种更新报告的方式相同，这里以查看更新状态摘要报告为例，操作步骤如下。

① 在“报告”窗口中单击“更新状态摘要报告”，显示如图 15-63 所示的“更新报告”窗口。其中包括更新级别、所属产品类型、计算机分组、更新执行结果等设置选项，用户可以选择要查看的更新类型和级别。

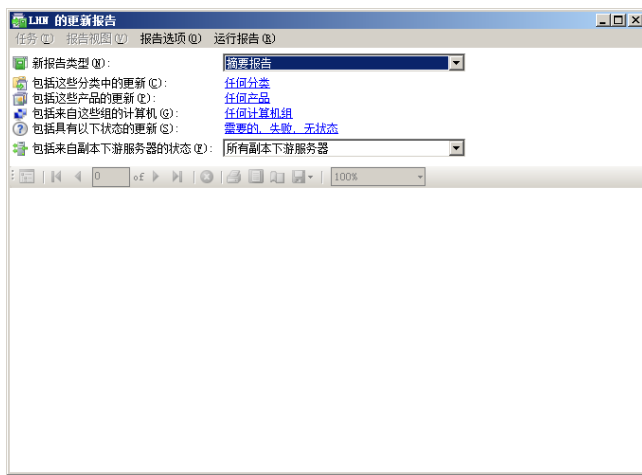


图 15-63 设置生成报告的更新属性

② 单击“运行报告”按钮开始生成报告，根据所选更新的不同生成报告所需的时间及内容也会有所不同。报告生成以后，显示如图 15-64 所示的“更新状态摘要报告”窗口。默认情况下，每页仅显示一项更新的相关信息，包括描述、分类、严重等级、编号，以及审批情况等。

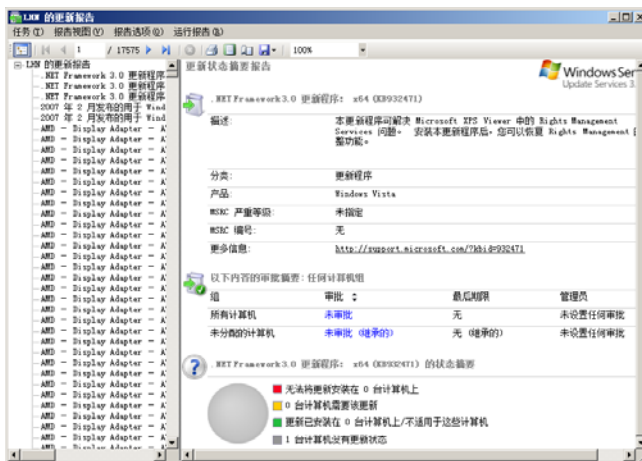
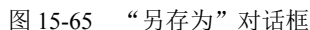


图 15-64 “更新状态摘要报告”对话框

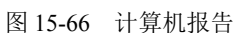
③ 为了便于日后查看更新报告，可以将报告导出为 Excel 或者 PDF 文件。以 Excel 文件为例，单击工具栏中的“导出”按钮。在下拉菜单中选择“Excel”选项，显示如图 15-65 所示的“另存为”对话框，输入一个文件名即可。



2. 计算机报告

在“报告”窗口中选择一种计算机报告，例如“计算机状态摘要”，打开“计算机报告”窗口。单击“运行报告”按钮，即可显示从 WSUS 服务器获取更新的客户端计算机信息，如图 15-66 所示，其中包括该计算机所使用的操作系统、语言、IP 地址，以及所安装的更新数量。

“同步报告”显示 WSUS 服务器的上次同步结果，或者特定时间段内的同步结果，用户可以查看有关这些更新的同步状态的详细信息。默认情况下，同步报告仅显示最近 30 天的同步结果，但可以根据需要选择不同的时间段来筛选报告结果。



506

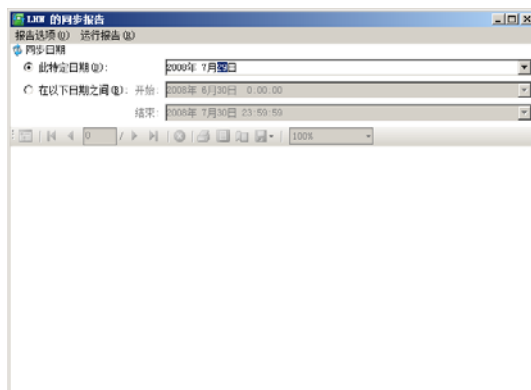


图 15-67 “同步报告”窗口

② 单击“运行报告”按钮开始生成报告，完成后显示曾经执行的同步操作及最新的更新，如图 15-68 所示。

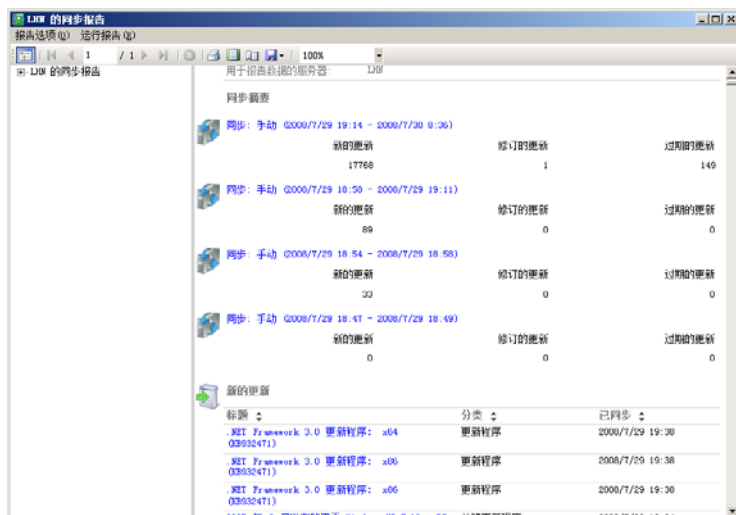


图 15-68 生成的报告

③ 如果要查看某一个同步的详细信息，则在“同步摘要”选项组中单击该同步。显示如图 15-69 所示的该次同步的时间及更新等。

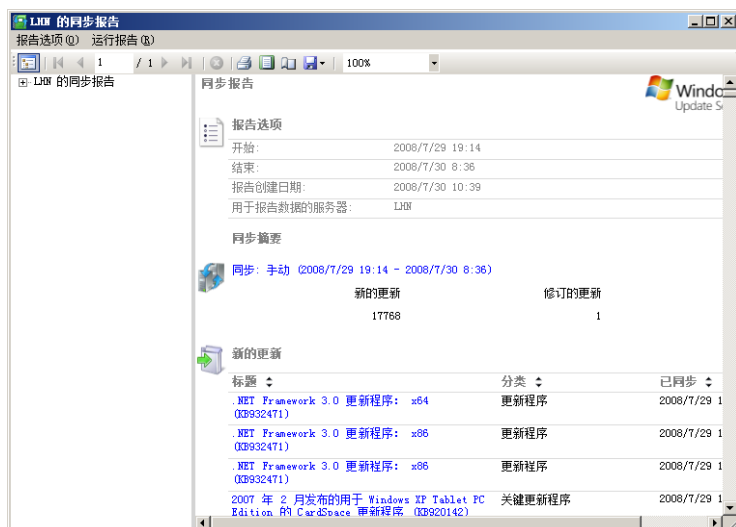


图 15-69 该次同步的时间及更新等

④ 如果要查看同步操作中某个更新的详细信息，可单击更新名称，显示如图 15-70 所示的“更新报告”窗口。在其中可以查看该更新的描述信息、所属类型及发布日期等信息，从而决定是否需要在客户端安装。

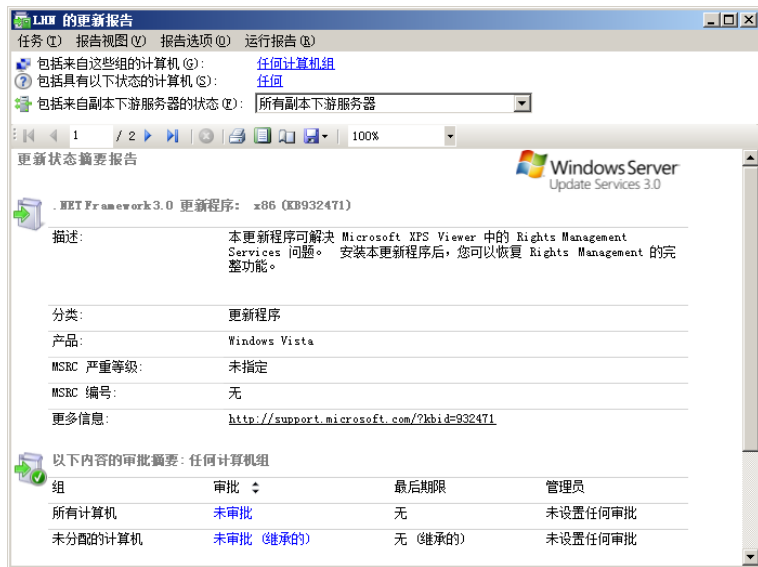


图 15-70 “更新报告”窗口

15.5 WSUS 服务器的选项

在安装 WSUS 过程中，通过 WSUS 配置向导即可完成 WSUS 的配置工作。也可以在安装 WSUS 后，在 WSUS 管理控制台中选择“选项”（如图 15-71 所示）来手动配置 WSUS 服务器，包括更新源和代理服务器、产品和分类、更新文件和语言、同步计划、自动审批、计算机、服务器清理向导、报告汇总、电子邮件通知，以及个性化等。

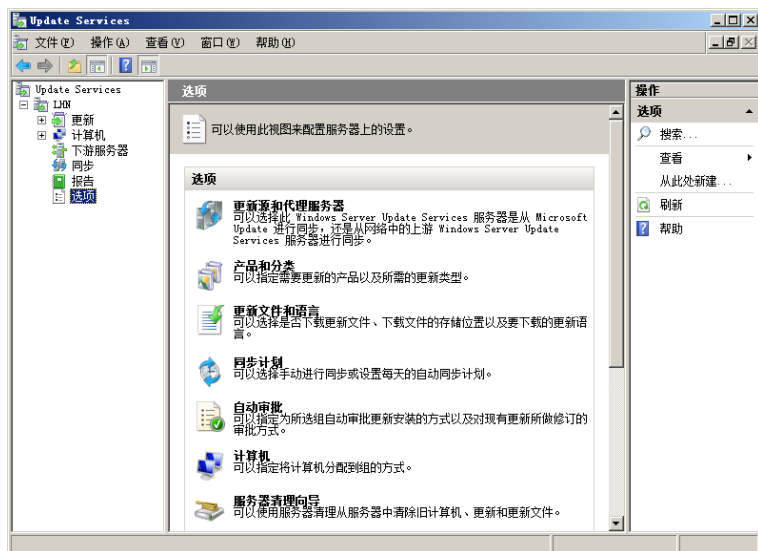


图 15-71 WSUS 选项

15.5.1 更新源和代理服务器设置

在 WSUS 控制台的“选项”窗口中，单击“更新源和代理服务器设置”链接，显示如图 15-72 所示的“更新源和代理服务器”对话框。在“更新源”选项卡中可以选择服务器从 Microsoft Update 服

服务器同步更新，还是从其他 WSUS 服务器同步更新。如果网络中使用了代理服务器，则可在“代理服务器”选项卡中设置。

需要注意的是，如果当前服务器正在进行同步，则无法更改更新方式，设置其他选项时也是如此。

15.5.2 产品和分类

如果需要指定需要同步更新的产品及所需要的类型，可单击“产品和分类”链接，显示如图 15-73 所示的“产品和分类”对话框。在“产品”下拉列表框中选择要更新的产品，在“分类”选项卡中则可选择要更新的类型。

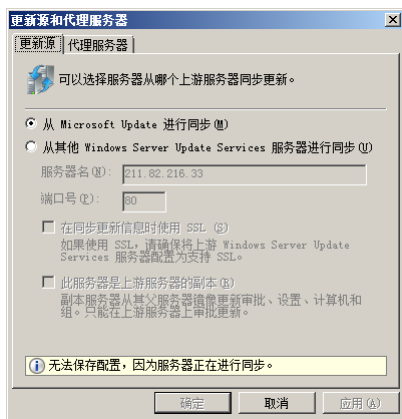


图 15-72 “更新源和代理服务器”对话框



图 15-73 “产品和分类”对话框

15.5.3 更新文件和语言

默认情况下，只有经过审批的文件 WSUS 才会将其下载到此服务器上。如果要指定更新文件的存储方式，可在 WSUS 的“选项”窗口中单击“更新文件和语言”超级链接，显示如图 15-74 所示的“更新文件和语言”对话框。默认选择“将更新文件本地存储在此服务器上”单选按钮，将更新文件存储在本地服务器中。如果要使更新文件不必审批即可下载到本地服务器上，则清除“仅当审批更新后才能将更新文件下载到本地服务器上”复选框。

打开“更新语言”选项卡，如图 15-75 所示，在其中可以选择要下载哪些语言的更新。

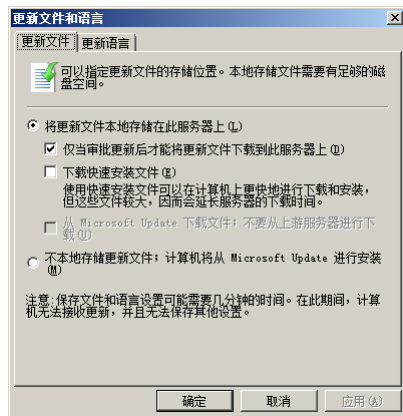


图 15-74 “更新文件和语言”对话框

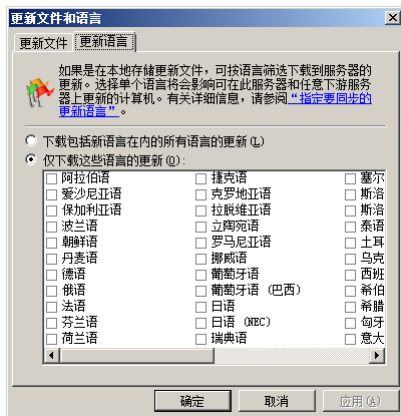


图 15-75 “更新语言”选项卡

15.5.4 同步计划

在 WSUS 的“选项”窗口中单击“同步计划”链接，显示如图 15-76 所示的“同步计划”对话框。在其中可以设置手动同步，还是自动同步。如果选择“手动同步”单选按钮，则必须由用户手动单击

“立即同步”才能进行同步；选择“自动同步”单选按钮并设置同步计划，可以让 WSUS 在规定的时间内自动进行同步。

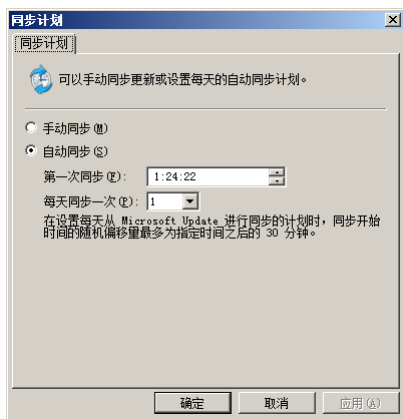


图 15-76 “同步计划”对话框

15.5.5 自动审批

默认情况下，WSUS 服务器不会自动审批任何更新，所有更新都必须由网络管理员手动审批完成。由于更新数量非常多，所以审批的工作量也非常大。如果使用自动审批功能，将特定的分类和产品类型的更新审批到指定的客户端，就可以大大减轻管理员的工作负担。不过，自动审批仅限于可靠性较高的更新。



提示

为避免安装更新之后可能导致的各种问题，建议审批之前进行严格测试，确认无误后审批到客户端。

在 WSUS 的“选项”窗口中单击“自动审批”链接，显示如图 15-77 所示的“自动审批”对话框，在其中可以设置自动批准规则。

现在创建一条审批规则，只允许 WSUS 自动审批 Windows Vista 操作系统的更新，操作步骤如下。

① 单击“新建规则”按钮，显示如图 15-78 所示的“添加规则”对话框。在“步骤 1：选择属性”列表框中选择用于批准的更新属于特定分类还是特定产品，当选中一种属性后，在“步骤 2：编辑属性”列表框中也会自动增加相应项的详细设置，在“步骤 3：指定名称”文本框中输入新规则的名称。

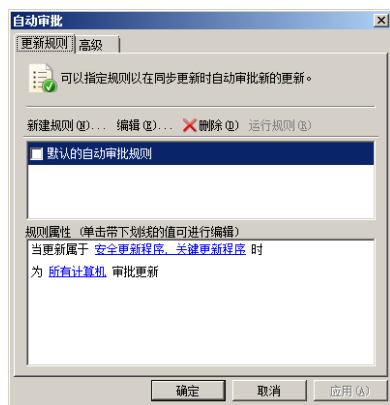


图 15-77 “自动审批”对话框

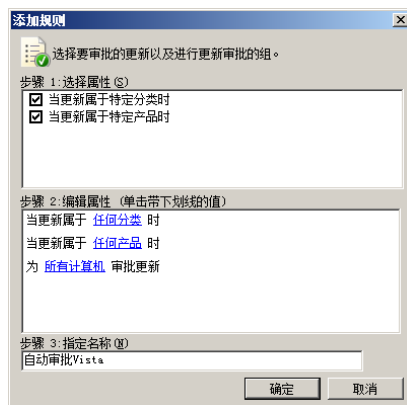


图 15-78 添加规则

② 在“步骤 2：编辑属性”列表框中编辑选定的分类，单击“任何分类”链接，显示如图 15-79 所示的“选择‘更新分类’”对话框。选择允许的分类，单击“确定”按钮保存设置。

③ 在“步骤 2：编辑属性”列表框中单击“任何产品”链接，显示如图 15-80 所示的“选择‘产

品’”对话框。选中“Windows Vista”复选框，单击“确定”按钮保存。

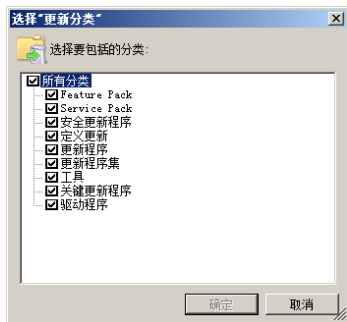


图 15-79 “选择‘更新分类’”对话框



图 15-80 “选择‘产品’”对话框

④ 在“步骤 2：编辑属性”列表框中单击“所有计算机”超级链接，显示如图 15-81 所示的“选择‘计算机组’”对话框。如果在 WSUS 中已将所有的 Windows Vista 计算机分到了一个组中，只需选中相应的计算机组即可；否则需选中“所有计算机”复选框。

⑤ 单击“确定”按钮保存设置，返回“自动审批”对话框，如图 15-82 所示。



图 15-81 “选择‘计算机组’”对话框

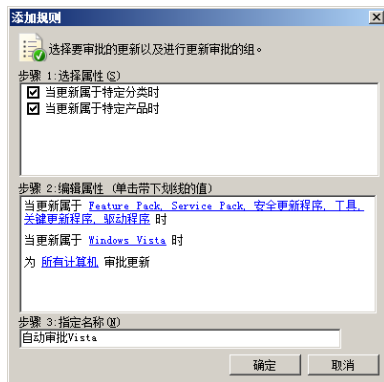


图 15-82 “自动审批”对话框

⑥ 单击“确定”按钮，一条用于自动审批 Vista 的规则创建完成，如图 15-83 所示。

⑦ 为了使新创建的审批规则立即生效，选中新规则。单击“运行规则”按钮，显示如图 15-84 所示的“运行规则”对话框，提示是否首先保存该规则。

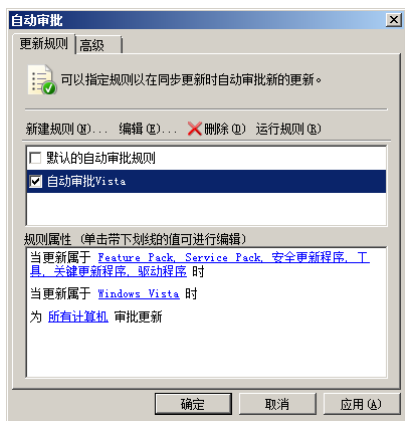


图 15-83 创建完成的规则

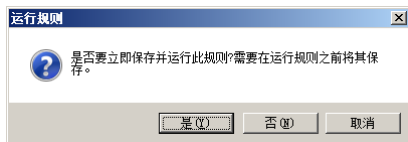


图 15-84 “运行规则”对话框

⑧ 单击“是”按钮，保存该规则并立即开始运行，显示如图 15-85 所示的“正在运行规则”对话框。此时 WSUS 服务器会根据自动审批规则中设置的条件筛选可用的更新安装程序，根据更新程序的数量不同，所需时间也不同，完成后显示已审批的更新数量。

⑨ 单击“关闭”按钮。

在“自动审批”对话框中，打开“高级”选项卡，如图 15-86 所示。默认情况下，系统自动审批 WSUS 产品本身更新及修订，并自动拒绝过期的更新。



图 15-85 “正在运行规则”对话框

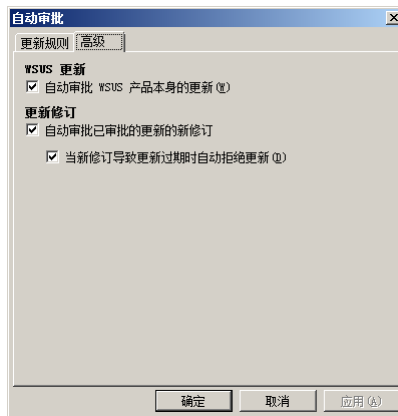


图 15-86 “高级”选项卡

15.5.6 分组计算机

通常情况下，网络管理员可以通过两种方法为计算机组分配计算机，即 WSUS 控制台和客户端策略。在 WSUS 的“选项”窗口中，单击“计算机”链接，显示如图 15-87 所示的“计算机”对话框，可以选择使用哪种方式为计算机分组。

15.5.7 服务器清理向导

WSUS 服务器运行一段时间以后，就会产生一些垃圾文件，例如过期的更新及无效的客户端等。这些文件不仅会占用大量磁盘空间，而且还可能造成服务器响应速度慢。从而影响分发效率，因此网络管理员需要对其进行清理。

(1) 在 WSUS 的“选项”窗口中单击“服务器清理向导”链接，运行 WSUS 服务器清理向导。首先显示如图 15-88 所示的“欢迎使用服务器清理向导”对话框，在其中可以选择想要清理的项目。

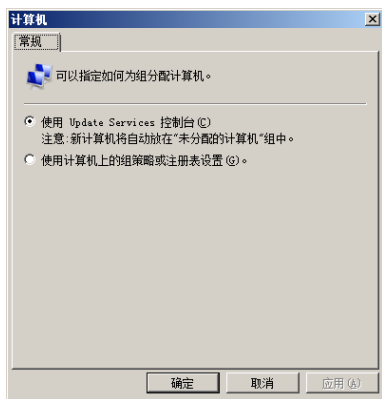


图 15-87 “计算机”对话框

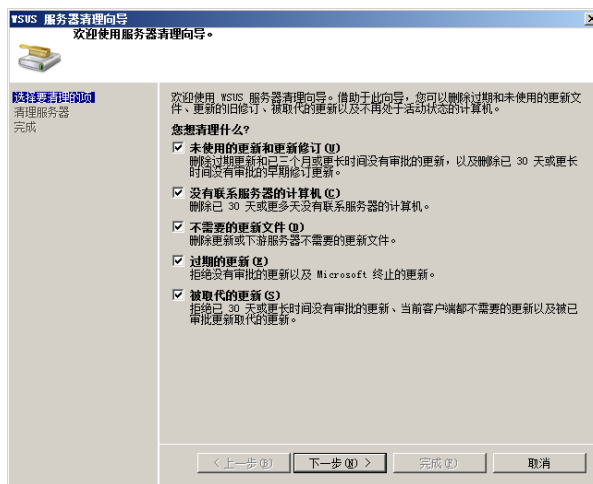


图 15-88 “欢迎使用服务器清理向导”对话框



在选择清理指定更新时要尤其注意查看其详细信息，确保已经过期或无用。

(2) 单击“下一步”按钮即可开始清理, 根据 WSUS 服务器的运行情况和所选的清理选项的不同, 需要的时间也会有所不同, 通常需要几分钟至十几分钟的时间。

(3) 清理完成后, 显示如图 15-89 所示的“清理完成”对话框。其中列出所清理的内容, 单击“完成”按钮退出即可。

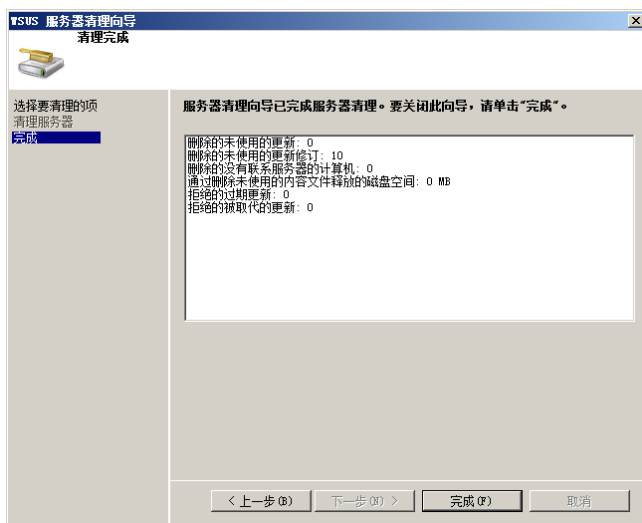


图 15-89 “清理完成”对话框

15.5.8 报告汇总

如果网络中存在下游 WSUS 服务器, 则可以设置是否让下游服务器将计算机和更新状态汇总到此服务器。

在 WSUS “选项” 窗口中单击“报告汇总”链接, 显示如图 15-90 所示的“报告汇总”对话框。系统默认选择“从副本下游服务器汇总状况”单选按钮, 即自动收集来自下游 WSUS 服务器的状态信息。如果不从下游服务器收集状态信息, 则可选择“不要从副本下游服务器汇总状态”单选按钮。

15.5.9 电子邮件通知

如果需要 WSUS 服务器在同步时第一时间通知网络管理员, 或者将状态报告发送给网络管理员, 则可以启用 WSUS 服务器的 E-mail 功能。

(1) 在 WSUS 的“选项”窗口中单击“电子邮件通知”链接, 显示如图 15-91 所示的“电子邮件通知”对话框。

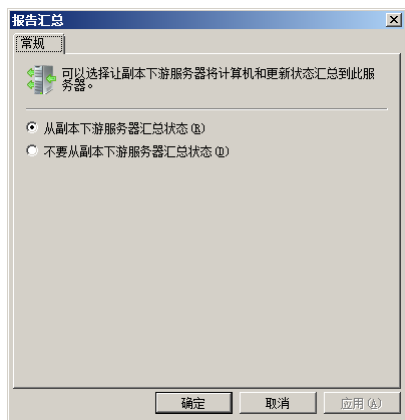


图 15-90 “报告汇总”对话框

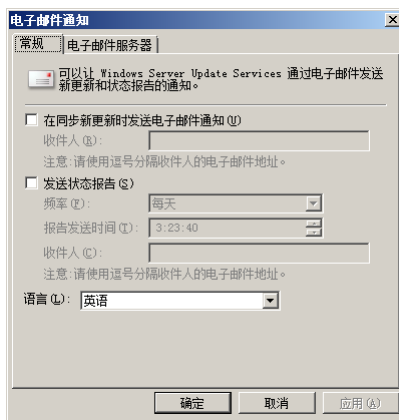


图 15-91 “电子邮件通知”对话框

(2) 在如图 15-92 所示的“常规”选项卡中选中“在同步新更新时发送电子邮件通知”复选框，在“收件人”文本框中输入收件人的 E-mail 地址。选中“发送状态报告”复选框，可设置发送频率和发送时间。如果将报告发送给多个用户，可在“收件人”文本框中同时输入多个 E-mail 地址，并以逗号分隔。在“语言”下拉列表框中选择电子邮件内容使用的语言。

(3) 打开如图 15-93 所示的“电子邮件服务器”选项卡，需要设置邮件服务器。由于发送邮件的过程是由 WSUS 服务器自动完成的，因此需要设置发送邮件时使用的用户名和邮件服务器地址。

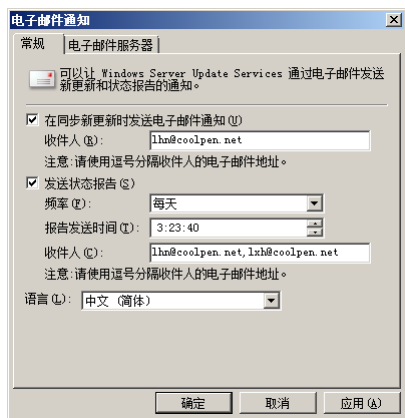


图 15-92 “常规”选项卡

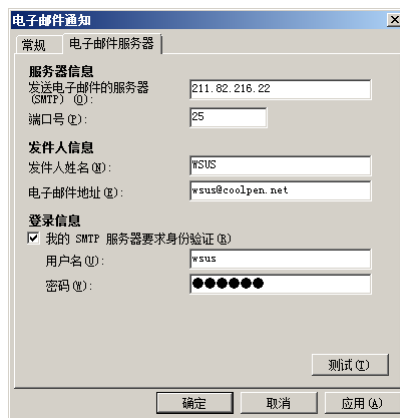


图 15-93 “电子邮件服务器”选项卡

(4) 设置完成后单击“确定”按钮保存设置。

15.5.10 WSUS 服务器配置向导

在安装 WSUS 时，默认会自动启动 WSUS 配置向导对 WSUS 进行一次配置。如果安装完成后还想利用配置向导设置，则在 WSUS 窗口中单击“WSUS 服务器配置向导”超级链接，启动配置向导。具体操作过程请参见前面所述内容，这里不再赘述。

第 16 章 网络策略和访问服务

远程访问是用户常用的方式，无论出差在外，还是在家办公，都可以通过 Internet 连接公司的内部网络。不过，Internet 传输的开放性很高，安全性较低。而通过利用 VPN（Virtual Private Network，虚拟专网）技术可以安全地连接到内部网络。但有些客户端由于未能及时安装更新并启用防火墙等，因此容易导致病毒和木马感染公司网络，影响网络的正常运行。利用网络访问保护（NAP）策略，可以将影响网络安全的计算机隔离到一个受限网络中，直至计算机修复达到网络健康标准后才允许接入。

16.1 路由和远程访问服务简介

路由和远程访问服务是 Windows Server 2003/2008 系统内置的服务，尤其是在 Windows Server 2008 中增加了网络策略功能来保护网络的安全。而所有 Windows 客户端都可以利用拨号或 VPN 方式来连接到内部网络中的远程访问服务器，从而访问网络中的资源。

➤➤ 16.1.1 远程访问服务器概述

Windows Server 2008 远程访问服务器支持远程访问通信协议和局域网通信协议，可以使远程客户端连接并访问本地网络的资源。配合使用 Windows Server 2008 访问策略，可以确保客户端的访问更加安全。

Windows Server 2008 远程访问服务器支持以下几种远程访问的通信协议。

（1）PPP 协议

PPP（Point-to-Point）是目前被广泛使用的远程访问通信协议，而且其安全措施优秀且扩充性较强，能够满足当前与未来的需求。

Windows Server 2008 远程访问服务器支持客户端利用 PPP 来连接。另外，Windows 2008/2003/XP/2000 等 Windows 客户端也支持利用 PPP 来拨号连接到支持 PPP 的远程访问服务器。

（2）SLIP 协议

SLIP（Serial Line Internet Protocol）是一个远程访问通信协议，通常在 UNIX 环境下使用。Windows Server 2008 的远程访问服务器并不支持客户端利用 SLIP 来连接，但是 Windows 操作系统的 VPN 客户端支持利用 SLIP 拨号连接到 SLIP 服务器。

（3）RAS 协议

Microsoft RAS Protocol 是 Microsoft 专有的通信协议，支持 NetBIOS 的标准。这个通信协议是旧版的操作系统所采用的远程访问通信协议，不过它只支持 NetBEUI 局域网通信协议，因此远程访问服务器与客户端都必须安装 NetBEUI 通信协议。

（4）ARAP 协议

ARP（Apple Remote Access Protocol）的 Macintosh 客户端可以通过此通信协议来连接 Windows Server 2008 远程访问服务器。但是 Windows Server 2008 作为 VPN 客户端时，不能够利用 ARAP 来连接支持 ARAP 的远程访问服务器。

16.1.2 NAP 概述

NAP (Network Access Protection, 网络访问保护) 可以提高移动计算机和内部网络的安全性, 网络管理员可以定义相应的防护策略。例如, 要求任何想访问网络的用户为操作系统打上最新的补丁, 并且安装反间谍软件和防病毒软件: 否则就无法访问网络。NAP 发现有问题的客户端之后, 自动地把该客户端隔离到一个受限制的网络中。以强制其安装最新的补丁程序, 或者将其完全同网络断开, 然后向用户发出帮助性提示。

NAP 不能取代其他网络安全机制, 根本无法阻止未授权用户访问网络。而是帮助保护网络, 以远离通过未打补丁或配置不当或未加保护的计算机连接到网络的授权用户带来的攻击和恶意软件。

1. NAP 组成

网络访问保护主要分为 4 部分即策略验证、隔离、补救和持续监控。

(1) 策略验证

策略验证指 NAP 根据网络管理员定义的一组规则评估系统及其状态的过程, NAP 在计算机尝试连接到网络时会使用安全健康程序和定义的策略相比较, 符合这些策略的计算机被视为状态良好的计算机; 而不符合其中一项或多项检查标准的计算机则被认为是状态不良的计算机。这些策略可以检查计算机是否安装有防病毒软件和反间谍软件、主机防火墙是否处于活动状态, 以及是否缺少某个安全更新等。

(2) 隔离

隔离可以理解为网络连接限制, 根据网络管理员定义的策略, NAP 可以将计算机的网络连接设置为各种状态。例如, 如果一台计算机因缺少关键的安全更新而被视为状态不良, 则 NAP 可以将该计算机置于隔离网络中。使其与网络中其他计算机隔绝, 直至恢复健康(安装补丁)为止。如果没有 NAP, 状态不良的客户端也可以不受限制地访问企业的网络。一旦恶意软件能够通过那些本该由更新程序修补的漏洞危害该计算机, 则可不断试图将自身感染的病毒传播给网络中的其他计算机。

NAP 有两种部署模式, 即监控模式和隔离模式。如果配置为监控模式, 即使发现授权用户的计算机不符合策略, 仍然可以访问网络。但不符合策略的状况会被记入日志, 网络管理员就可以指导用户如何让计算机符合策略; 如果配置为隔离模式, 不符合策略的计算机只能有限地访问网络, 可以在该网络中找到符合策略的资源。

(3) 补救

对于已经限制连接并不处理那些状态不良的计算机, NAP 提供了补救策略, 被隔离的计算机无需网络管理员干预即可纠正影响运行状态的问题。受限的网络允许状态不良的计算机访问安装缺少更新程序必需的特定网络资源, 例如 Windows Server Update Services 服务器。即有了 NAP, 状态不良的计算机只能访问那些可使其运行正常的网络资源, 在其恢复健康前不能访问网络中的其他计算机。

(4) 持续监控

持续监控即强制计算机在与网络保持连接期间, 而不仅仅在初始连接时始终监控这些可保持状态良好的策略。如果该计算机状态与策略不相符合, 例如禁用了 Windows 防火墙, 则 NAP 将自动开启防火墙, 直至恢复正常状态后方可访问网络。

2. 网络访问

NAP 提供了多种控制网络访问的技术, 802.1X 在网络硬件层提供基于端口的访问控制、基于 IPsec 的强制技术和基于 DHCP 的强制技术。

DHCP 服务器为运行状态不良的客户端提供来自受限的 IP 租约, 这些租约使用单独的 DNS 后缀和 IP 路由来控制受限客户端可以访问的资源。如果要使用 DHCP 强制技术, 服务器端必须使用 Windows Server 2008 的 DHCP 服务角色。Windows Vista 操作系统中内置了 NAP 支持, Windows XP 的 SP3 版

本支持 NAP 网络访问保护。

对许多中小型企业来说,实施基于 DHCP 的 NAP 强制技术是最快且最简单的可选方案,因为这种技术不需要对网络进行其他更改。而且除 DHCP 服务和 NPS 服务之外,不需要其他服务。尽管 IPsec 和 802.1X 强制方案更灵活,但它们都需要在网络中进行额外更改并部署新的服务。

16.1.3 VPN 服务概述

VPN 是一种通过公共网络(比如 Internet)把两个私有网络连接在一起的技术,它允许用户通过安全廉价的方法把家庭计算机与公司网络连接在一起,这种通过 Internet 的连接方式要比专线便宜得多。使用 VPN 时,由于与专用网络安全连接时利用的是公共 Internet,而非长途电话呼叫,因此可以节省费用。

1. 软件 VPN 和硬件 VPN

根据实现方式的不同,VPN 可以分为软件 VPN 和硬件 VPN。

(1) 软件 VPN

软件 VPN 顾名思义即通过软件实现的 VPN 安全连接,专业的软件 VPN 产品不仅可以完全独立于 VPN 硬件设备之外,而且功能强大且操作简便。更重要的是可以节省大部分投资,有些软件甚至是完全免费的。

VPN 软件的安装和普通应用程序没有区别,通常采用客户端/服务器模式。其实,Windows 2000/2003/2008 系统集成的 PPTP 的 VPN 就是一款非常不错的软件,在不增加任何成本的情况下就可以享受到安全且可靠的 VPN 连接。

目前,一些主流厂商的 VPN 软件安全性也有了很大的提高,如国内的联想网御和北京金万维等。这些产品价格均在千元左右,是广大中小用户的首选。国外知名度较高的 VPN 软件公司技术更加成熟,如 Check Point 的 VPN 软件产品,价格为几万~几十万不等,适用于大型企业。

(2) 硬件 VPN

硬件 VPN 是目前应用较多的 VPN 技术,其突出特点是安全性高。并且随着网络技术的不断发展,许多常规网络产品,如路由器、防火墙中都集成了 VPN 功能。在增加一小部分成本的情况下,即可拥有硬件级的 VPN 安全保障,可谓是一举多得。另外,有些网络设备的设计更加人性化,提供了可扩展的 VPN 模块插槽。需要时用户只需购买与之匹配的 VPN 功能模块,插入插槽即可使用,这也是硬件 VPN 技术的一种。

作为增值服务“赠送”的 VPN 服务的部署,往往需要借助其主硬件的管理系统实现,如 Cisco 7600 系列路由器的 VPN 功能需要在其 IOS 中配置。

专业 VPN 硬件的性能相对上述作为附属功能的 VPN 硬件技术又上了一个台阶,VPN 技术的主要目标就是保障连接安全,使用过软件 VPN 的用户可能体会到如果安全级别太高,处理速度就会下降,传输速度也会降低。如果一味追求处理速度和传输速率,安全性又难以保障。专业的 VPN 硬件正是在这种情况下应运而生的,通过专业的硬件设备进行高级别加密和信息处理。如 Cisco VPN 3080 系列集中器支持 3DES 加密技术,加密吞吐量高达 1.9 Gb/s,并且同时可提供其他附属功能。需要注意的是这类产品的价格非常昂贵,如 Cisco VPN 3080 的官方报价一直在 10 000 美元左右,适用于安全性及处理效率要求较高的大型企业用户。

2. VPN 的特点

要实现 VPN 连接,局域网内必须首先建立一台 VPN 服务器。该服务器必须拥有一个公共 IP 地址,一方面连接企业内部的专用网络;另一方面用来连接到 Internet。当客户端通过 VPN 连接与专用网络中的计算机通信时,首先由 ISP 将所有数据传送到 VPN 服务器,然后再由 VPN 服务器负责将所有数据传送到目标计算机。VPN 具有以下特点。

(1) 费用低廉

远程用户可以接入 Internet, 以其作为通道与企业内部专用网络相连接。从而大大降低了通信费用, 而且企业可以节省购买和维护通信设备的费用。

使用 VPN, 远程用户可以通过 Internet 访问公司的局域网 (LAN), 而费用只是传统的远程访问方案的一小部分。可以使用网络适配器拨入 VPN, 就像通过调制解调器连接到传统的远程服务器一样, VPN 使公司不必花钱购买和维护诸如调制解调器和专用模拟电话线之类的组件。调制解调器及其相关的基础设备仍然集中在 Internet 服务提供商所在的位置, 而不必牺牲安全性或控制远程连接的能力。同时, 通过其他 VPN 所必需的已验证的访问、加密和用户数据压缩可以确保安全地访问专用数据。

(2) 安全性高

VPN 使用 3 个方面的技术 (通信协议、身份验证和数据加密) 保证了通信的安全性, 当客户端向 VPN 服务器发出请求时, VPN 服务器响应请求并向客户端发出身份质询。然后客户端将加密的响应信息发送到 VPN 服务端, VPN 服务器根据数据库检查该响应。如果账户有效, VPN 服务器将检查该用户是否具有远程访问的权限。如果有, VPN 服务器接受此连接。在身份验证过程中产生的客户端和服务器的公有密钥将用来加密数据。

(3) 支持常用的网络协议

由于 VPN 支持常用的网络协议, 所以诸如以太网、TCP/IP 和 IPX 网络上的客户可以很容易地使用 VPN。不仅如此, 任何支持远程访问的网络协议在 VPN 中也同样被支持。这意味着可以远程运行依赖于特殊网络协议的程序, 因此可以减少安装和维护 VPN 连接的费用。

(4) 有利于 IP 地址安全

VPN 在 Internet 中传输数据时是加密的, Internet 上的用户只能看到公共的 IP 地址。而看不到数据包内包含的专用网络地址, 因此保护了 IP 地址的安全。

(5) 网络架构弹性大

VPN 较专线式的架构更有弹性, 可以轻易地扩充网络或变更网络架构 (增加端口及更换用户端设备)。VPN 支持通过 Intranet 和 Extranet 的任何类型的数据流, 方便增加新的节点。并支持多种类型的传输媒介, 可以满足同时传输语音、图像和数据等新应用对高质量传输及带宽增加的需求。

(6) 管理方便灵活

架构 VPN 只需较少的网络设备及物理线路, 使网络的管理变得较为轻松。不论分公司或远程访问用户, 均只需通过一个公用网络端口或 Internet 的路径即可进入企业网络。公用网承担了网络管理的重要工作, 关键任务可获得所必须的带宽。

(7) 完全控制主动权

VPN 使企业可以利用 NSP (网络服务提供商) 的设施和服务, 同时又完全掌握自己网络的控制权。例如, 企业可以把拨号访问交给 NSP 处理, 由自己负责用户的验证、访问权、网络地址、安全性和网络变化管理等重要工作。

16.2 配置和管理远程访问服务

利用远程访问服务器, 客户端可以利用拨号或 VPN 方式来远程连接到局域网内部的服务器, 并访问其中的资源。而 VPN 方式由于安全、速度快且设置简单等优点, 成为当前最常用的连接方式, 而拨号方式已基本被淘汰。

16.2.1 配置准备工作

在配置远程访问服务器之前, 应事先做好各种准备工作。例如, 加入域、安装并配置 DHCP 服务器等。同时远程访问服务器中需要安装两块网卡, 一块网卡设置内网地址, 用来连接局域网; 另一块

设置公网地址，用来连接 Internet。

1. 设置 IP 地址

① 单击“开始”→“控制面板”→“网络和共享中心”选项，打开“网络和共享中心”窗口。单击“管理网络连接”超级链接，显示如图 16-1 所示的“网络连接”窗口，用来设置两块网卡的 IP 地址。

② 选择连接局域网的本地连接，右击选择快捷菜单中的“属性”选项，显示如图 16-2 所示的“本地连接 属性”对话框。

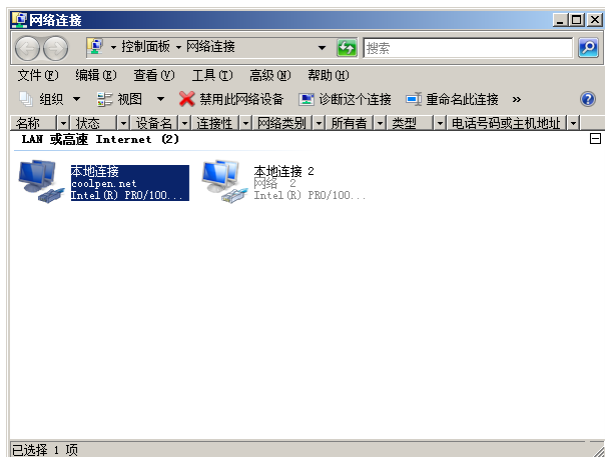


图 16-1 “网络连接”窗口

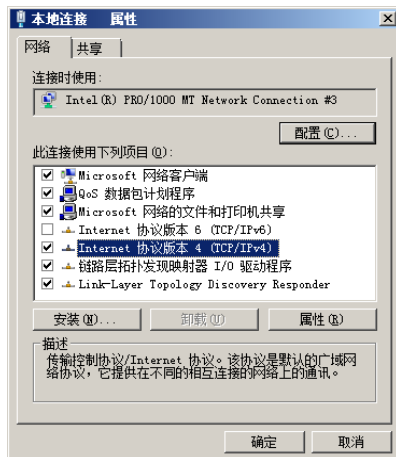


图 16-2 “本地连接 属性”对话框

③ 选择“Internet 协议版本 4 (TCP/IPv4)”选项，单击“属性”按钮，显示其属性对话框。设置局域网的 IP 地址，如图 16-3 所示，其中 DNS 服务器地址要设置为域控制器的 IP 地址。

④ 同时，另一个连接 Internet 的本地连接要设置为可以连接 Internet 的外网 IP 地址，如图 16-4 所示。

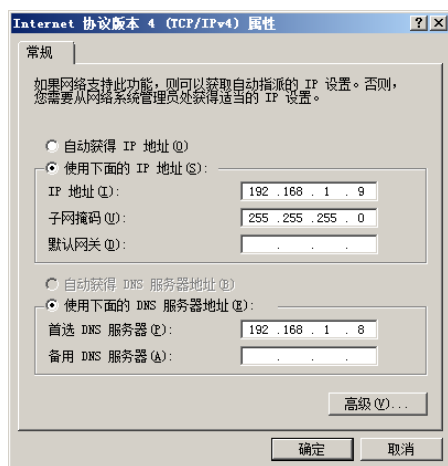


图 16-3 设置局域网 IP 地址

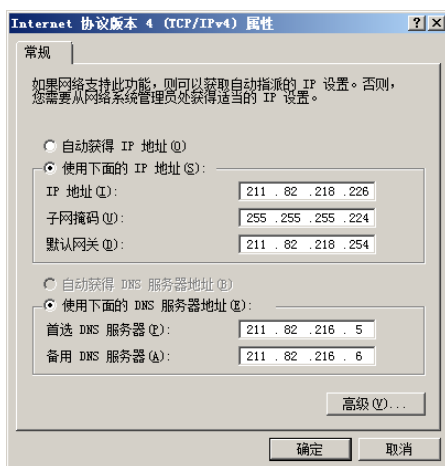


图 16-4 设置外网 IP 地址

2. 加入域

① 右击“计算机”选项，在快捷菜单中的选择“属性”选项，显示如图 16-5 所示的“系统”窗口。

② 单击“改变设置”超级链接，显示如图 16-6 所示的“系统属性”对话框。

③ 单击“更改”按钮，显示如图 16-7 所示的“计算机名/域更改”对话框。选择“域”单选按钮，并输入域名。



图 16-5 “系统”窗口

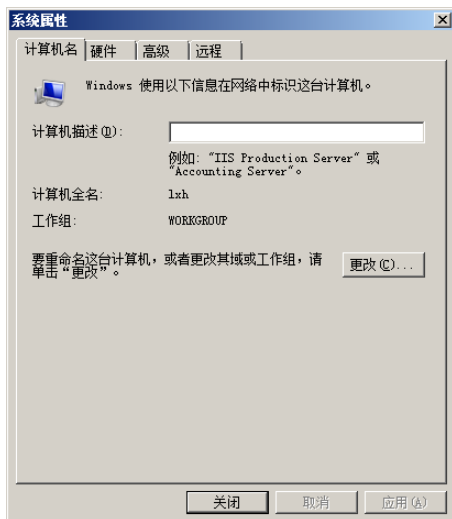


图 16-6 “系统属性”对话框

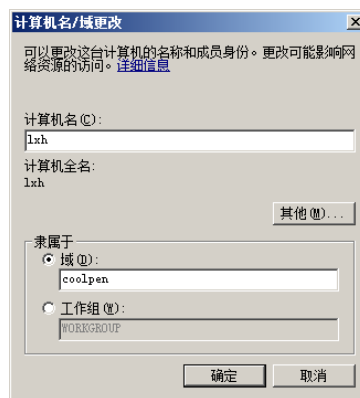


图 16-7 “计算机名/域更改”对话框

④ 单击“确定”按钮，显示如图 16-8 所示的“Windows 安全”对话框，在“用户名”和“密码”文本框中输入具有加入域权限的用户名和密码。

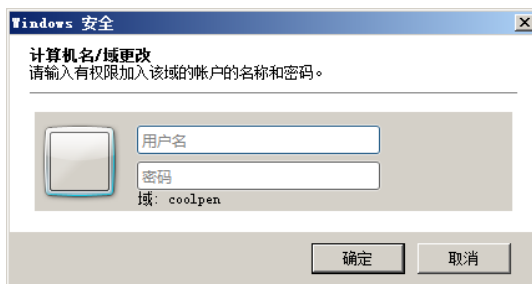


图 16-8 “Windows 安全”对话框

⑤ 单击“确定”按钮即可加入域，根据系统提示重新启动系统，使用域用户账户登录即可。

3. 安装并设置 DHCP 服务器

将服务器加入域并重新启动，使用域成员身份登录后安装 DHCP 服务器并创建作用域，然后即可

配置网络访问保护。

(1) DHCP 服务器安装完成以后, 打开 DHCP 控制台, 如图 16-9 所示。

(2) 展开“IPv4”选项, 右击作用域。选择快捷菜单中的“属性”选项, 显示作用域的属性对话框。打开如图 16-10 所示的“网络访问保护”选项卡, 选择“对此作用域启用”单选按钮, 启用网络访问保护功能。

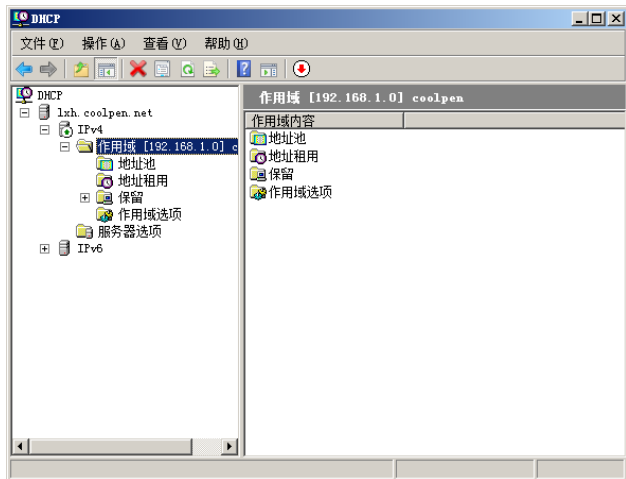


图 16-9 DHCP 控制台

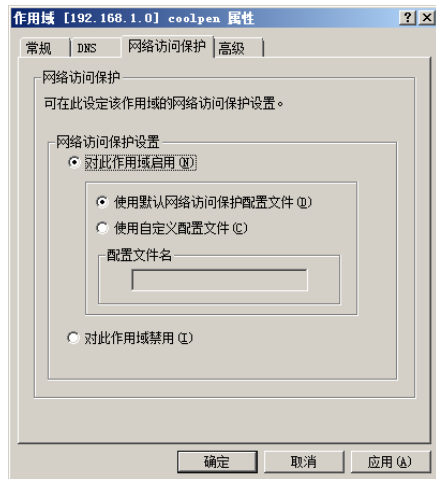


图 16-10 “网络访问保护”选项卡

(3) 单击“确定”按钮。

16.2.2 配置远程访问服务

远程访问服务器中需要安装两块网卡, 一块设置内网地址, 用来连接局域网; 另一块设置公网地址, 用来连接 Internet。同时为了便于客户端配置 IP 地址, 网络中应安装 DHCP 服务器。

1. 安装远程访问服务

① 运行“添加角色向导”链接, 在如图 16-11 所示的“选择服务器角色”对话框中选择“网络策略和访问服务”角色。

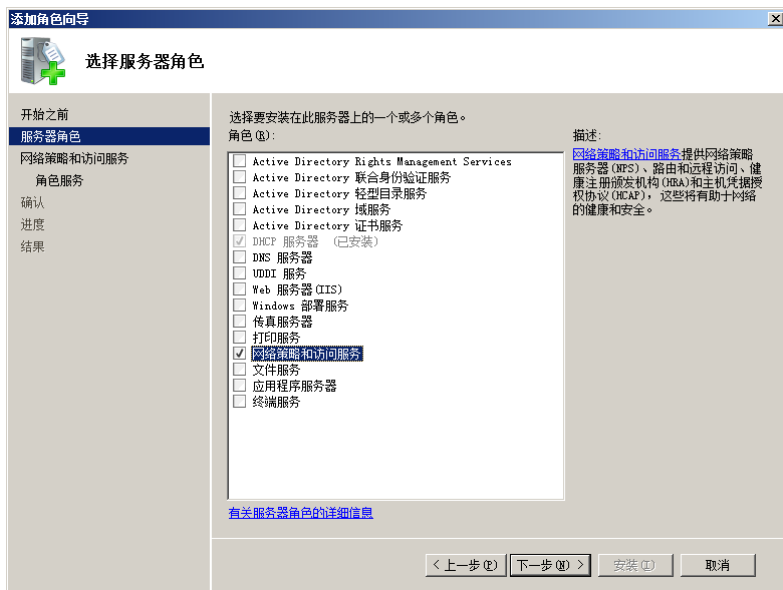


图 16-11 “选择服务器角色”对话框

② 单击“下一步”按钮，显示如图 16-12 所示的“网络策略和访问服务”对话框，其中显示网络策略和访问服务的简介信息。

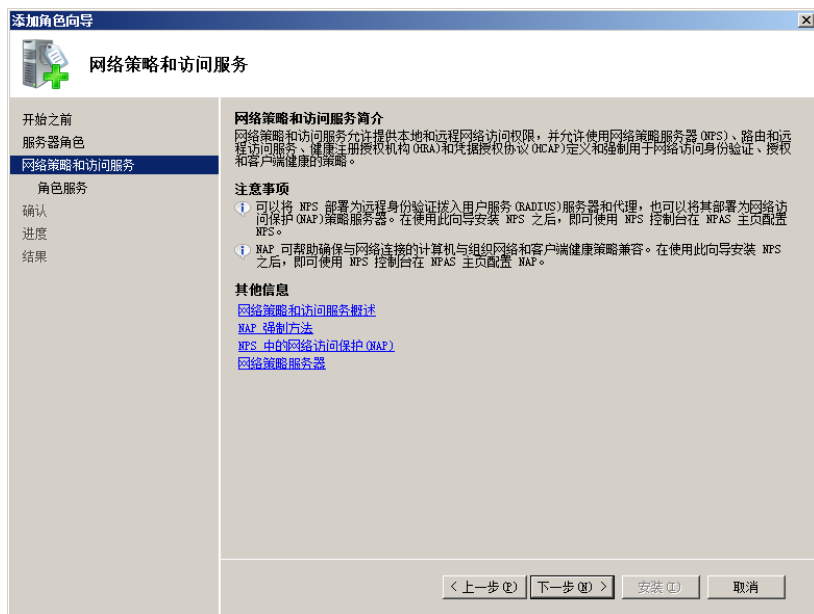


图 16-12 “网络策略和访问服务”对话框

③ 单击“下一步”按钮，显示如图 16-13 所示的“选择角色服务”对话框，选中“网络策略服务器”和“路由和远程访问服务”复选框。

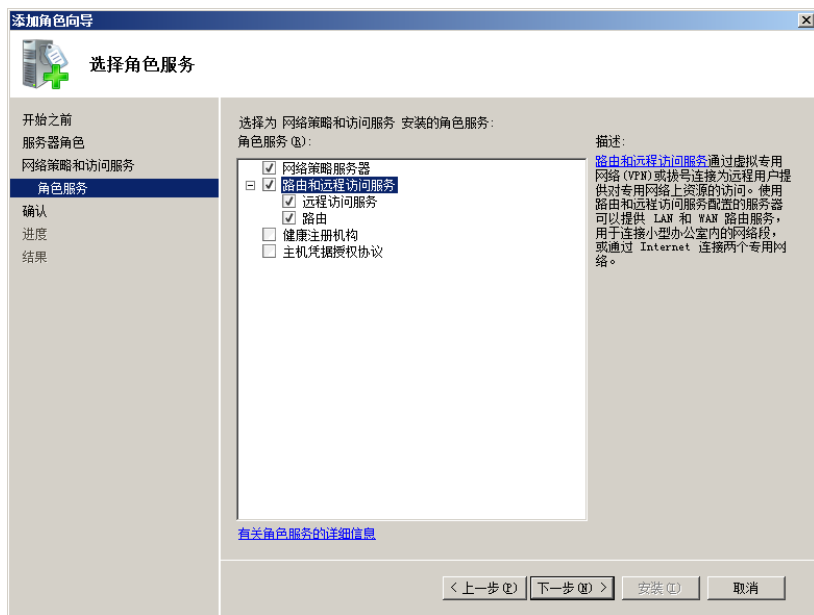


图 16-13 “选择角色服务”对话框

④ 单击“下一步”按钮，显示如图 16-14 所示的“确认安装选择”对话框，其中显示将要安装的角色。

⑤ 单击“安装”按钮开始安装。完成后显示如图 16-15 所示的“安装结果”对话框。

⑥ 单击“关闭”按钮，安装完成远程访问服务。



图 16-14 “确认安装选择”对话框



图 16-15 “安装结果”对话框

2. 配置路由和远程访问服务

远程访问服务安装完成后即可启用路由和远程访问功能。

- ① 单击“开始”→“管理工具”→“路由和远程访问”选项，打开“路由和远程访问”窗口，如图 16-16 所示，默认未启用路由和远程访问功能。
- ② 右击服务器名并选择快捷菜单中的“配置并启用路由和远程访问”选项，打开“路由和远程访问服务器安装向导”对话框，如图 16-17 所示。
- ③ 单击“下一步”按钮，显示如图 16-18 所示的“配置”对话框。其中提供多种方式来实现远程访问，这里选择“远程访问（拨号或 VPN）”单选按钮。

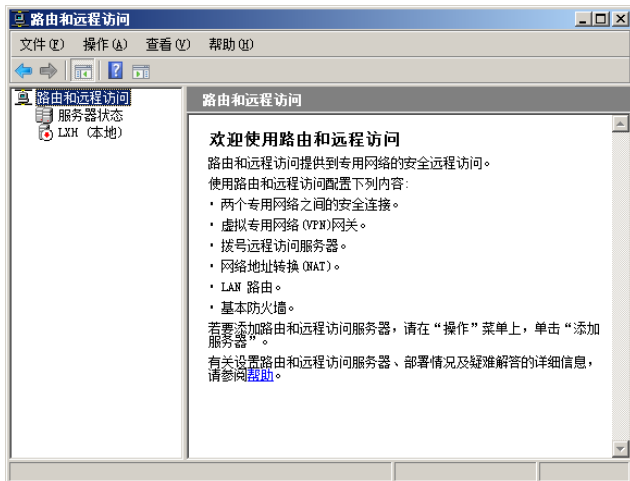


图 16-16 “路由和远程访问”窗口

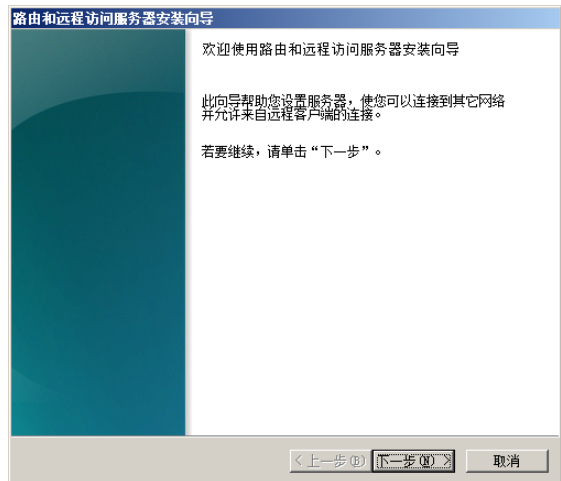


图 16-17 “路由和远程访问服务器安装向导”对话框

④ 单击“下一步”按钮，显示如图 16-19 所示的“远程访问”对话框。由于使用 VPN 连接，因此选中“VPN”复选框，使远程客户端可以通过 Internet 利用 VPN 拨号连接到此服务器。

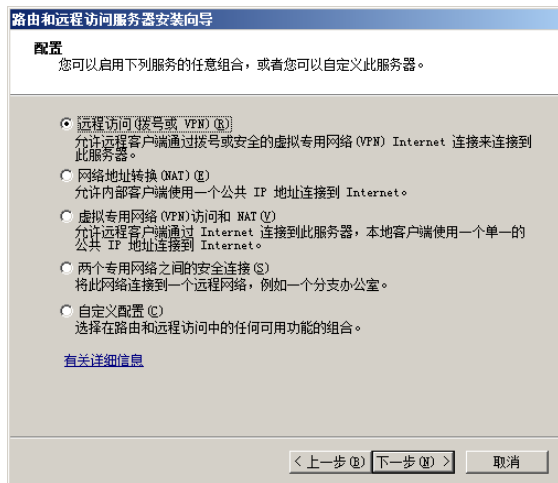


图 16-18 “配置”对话框

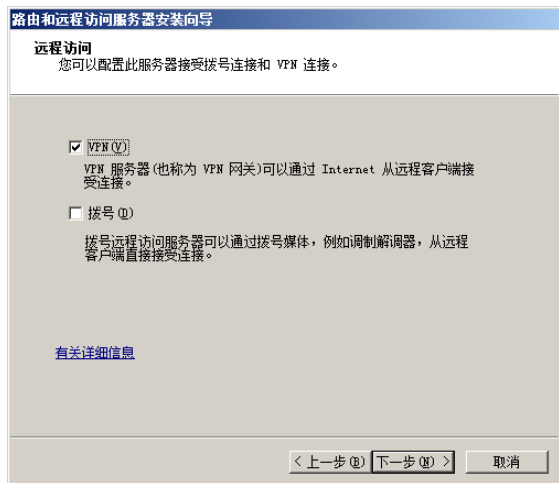


图 16-19 “远程访问”对话框

⑤ 单击“下一步”按钮，显示如图 16-20 所示的“VPN 连接”对话框。在“网络接口”列表框中选择此服务连接到 Internet 的连接即可。

⑥ 单击“下一步”按钮，显示如图 16-21 所示的“IP 地址分配”对话框，在其中指定远程客户端获得 IP 地址的方式。由于网络中已经配置 DHCP 服务器，因此选择“自动”单选按钮，使客户端自动从 DHCP 服务器获得 IP 地址。

⑦ 单击“下一步”按钮，显示如图 16-22 所示的“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，则添加 RADIUS 服务器非常有用；否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求身份验证。

⑧ 单击“下一步”按钮，显示如图 16-23 所示的“正在完成路由和远程访问服务器安装向导”对话框。其中的“摘要”下拉列表框中显示当前所做的设置，单击“上一步”按钮可返回修改。

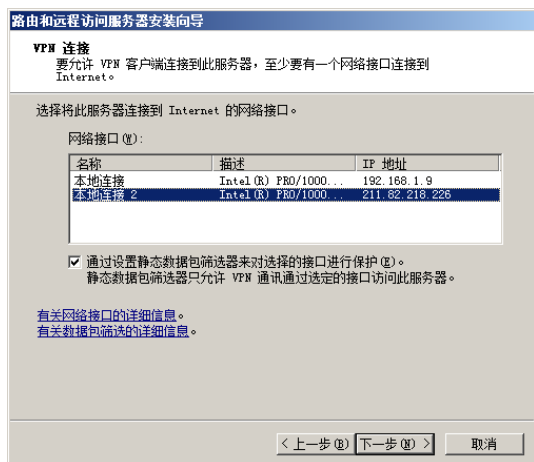


图 16-20 “VPN 连接” 对话框

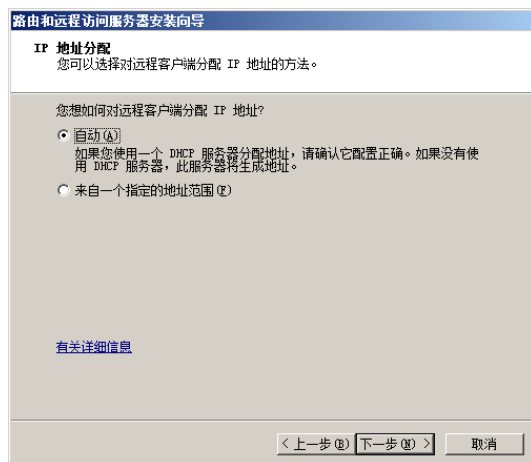


图 16-21 “IP 地址分配” 对话框

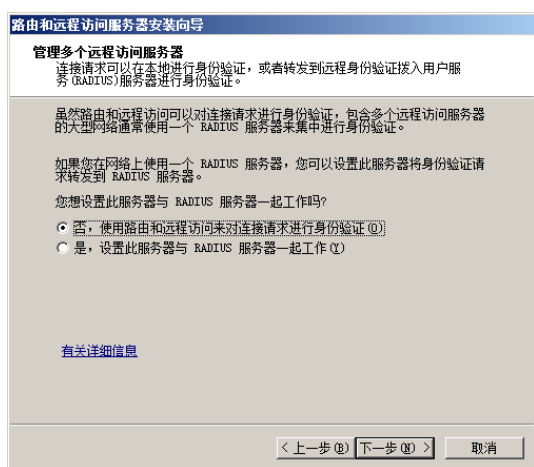


图 16-22 “管理多个远程访问服务器” 对话框

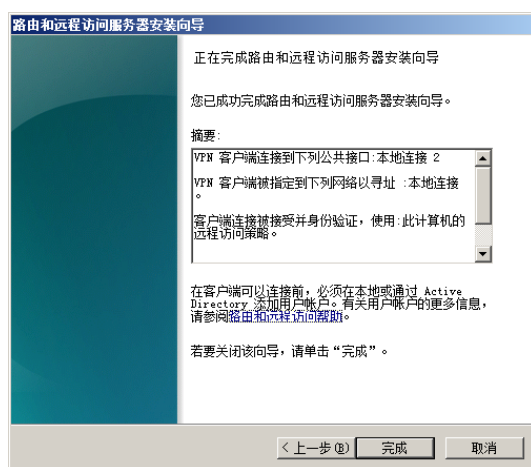


图 16-23 “正在完成路由和远程访问服务器安装向导” 对话框

9 单击“完成”按钮，显示如图 16-24 所示的提示框。

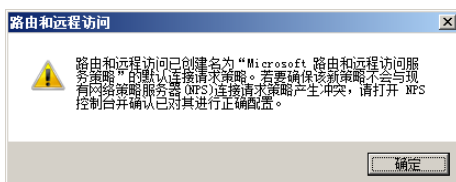


图 16-24 提示框

10 单击“确定”按钮，显示如图 16-25 所示的“路由和远程访问”对话框。提示用户在设置远程访问服务器以后，需要指定 DHCP 服务器的 IP 地址。

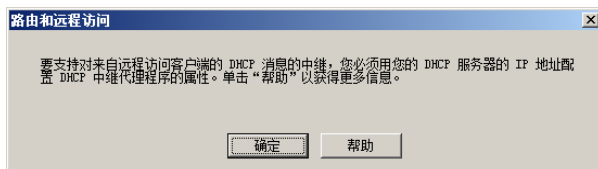


图 16-25 提示框

11 单击“确定”按钮，启动路由和远程访问功能。返回“路由和远程访问”控制台，如图 16-26 所示。此时，如果要转发 DHCP 消息，可通过“IPv4（或 IPv6）”→“DHCP 中继代理程序”选项来完成。

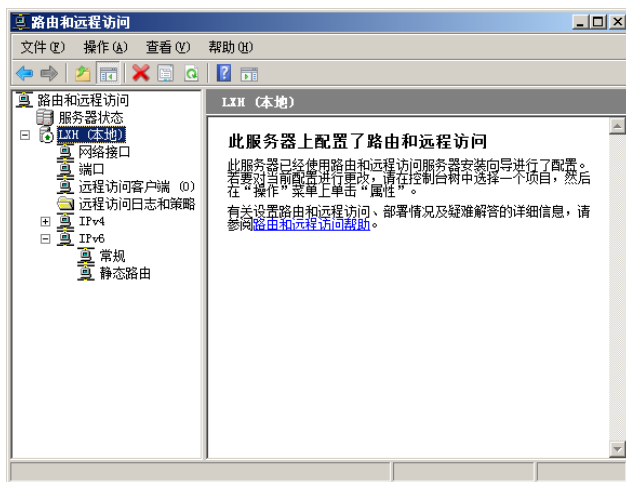


图 16-26 “路由和远程访问”控制台

16.2.3 设置 VPN 服务器

VPN 是客户端计算机访问远程访问服务器的最常用的方式，不仅传输安全，而且设置简单且速度快。在 Windows Server 2008 路由和远程访问服务器中，如果允许客户端以 VPN 方式连接，则表示已经将服务器配置为 VPN 服务器。

1. 赋予用户拨入权限

默认状态下，VPN 服务器禁止所有用户拨入，系统管理员需要对特定用户账户赋予访问权限；否则将无法正常使用。操作步骤如下。

① 单击“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开“Active Directory 用户和计算机”窗口，如图 16-27 所示。

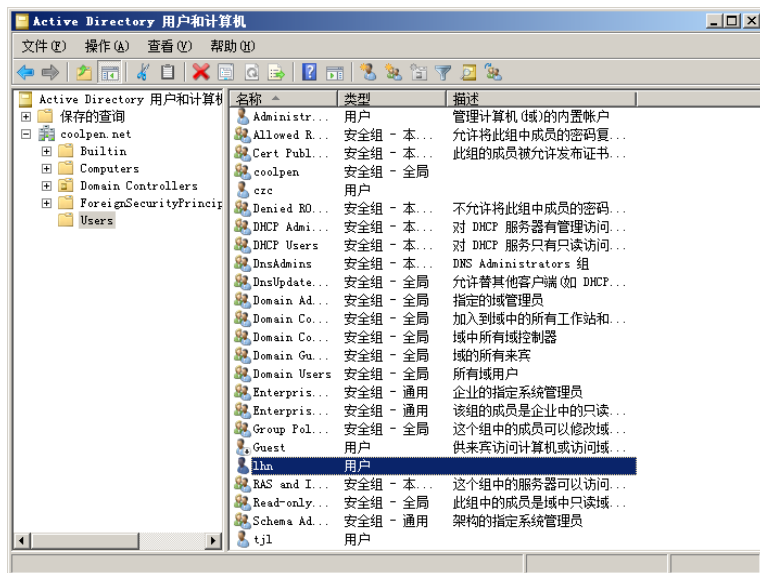


图 16-27 “Active Directory 用户和计算机”窗口

② 选择需要设置拨入权限的用户账户，右击并选择快捷菜单中的“属性”选项，显示该用户的属性对话框。打开如图 16-28 所示的“拨入”选项卡，在“网络访问权限”选项组中选择“允许访问”单选按钮。

③ 单击“确定”按钮保存设置，执行同样步骤可继续为其他用户启用拨入功能。



提示

“通过 NPS 网络策略控制访问”要求 VPN 客户端必须通过本地服务器或当前网络中的网络策略服务器的身份验证才可以拨入，与 Windows Server 2003 中的“通过远程访问策略控制访问”功能类似。没有配置 NPS 的用户，则直接选择“允许拨入”单选按钮即可。

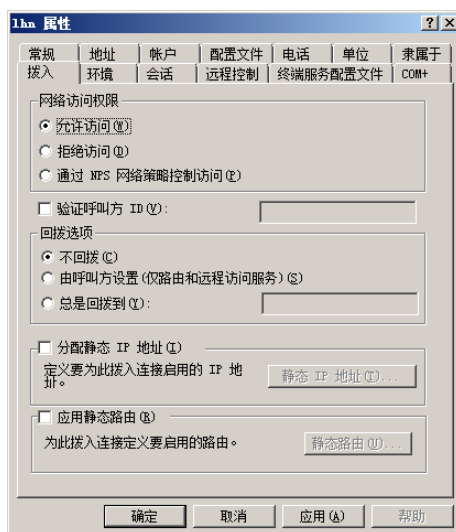


图 16-28 “拨入”选项卡

2. 设置服务器端口

将“路由和远程访问”服务器配置成 VPN 服务器时，默认创建 128 个 PPTP 虚拟端口、128 个 L2TP 虚拟端口和 128 个 SSTP 虚拟端口。其中 SSTP 协议是微软公司为 Vista 和 Windows Server 2008 开发的一种远程访问隧道协议，它可以创建一个在 HTTPS 上传送的 VPN 隧道。使用户设备能够安全地从 Internet 上的任何地点访问网络，完全不需要担心常见的端口阻拦问题。目前主要应用的是 PPTP 和 L2TP 两种虚拟端口。

(1) 在“路由和远程访问”窗口中选择“端口”选项，即可看到所有的虚拟端口，如图 16-29 所示。

(2) 右击“端口”并选择快捷菜单中的“属性”选项。打开“端口 属性”对话框，如图 16-30 所示。其中显示“路由和远程访问”使用的设备，可以配置 PPTP 端口和 L2TP 端口。

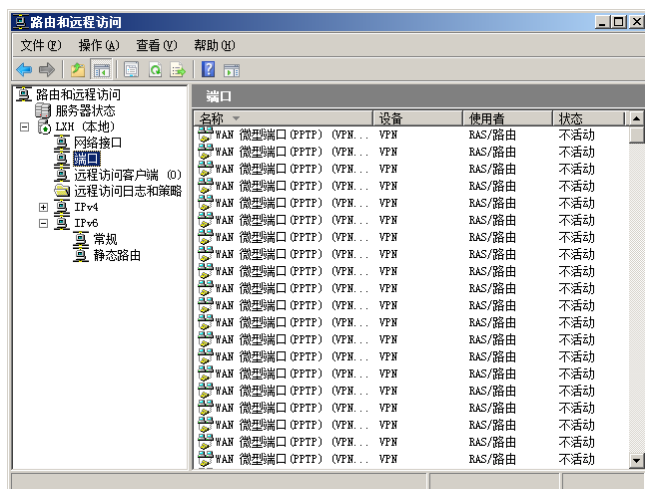


图 16-29 所有的虚拟端口

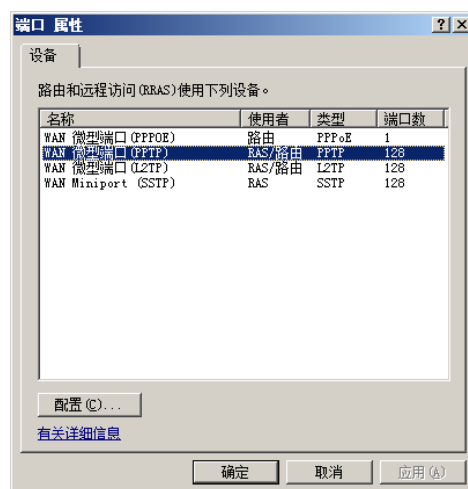


图 16-30 “端口 属性”对话框

(3) PPTP 和 L2TP 端口只是所使用的协议不同,但配置方式相同,这里以 PPTP 端口的设置为例说明。选择“WAN 微型端口 (PPTP)”选项,单击“配置”按钮,显示如图 16-31 所示的“配置设备 - WAN 微型端口 (PPTP)”对话框,其中的选项如下。

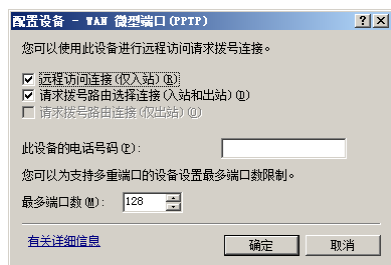


图 16-31 “配置设备 - WAN 微型端口 (PPTP)”对话框

远程访问连接 (仅入站): 表示允许远程客户端拨入,在远程访问服务器必须选中该复选框。

请求拨号路由选择连接 (入站和出站): 使用 VPN 服务器连接两个远程的局域网时,需使用该复选框。

请求拨号路由连接 (仅出站): 通过共享拨号的方式连接到另外一个网络时,使用该复选框。

此设备的电话号码: 输入此设备连接的电话号码,通常只在配置调制解调器的端口时使用。

最多端口数: 每一个端口数提供一个远程的连接,默认设置为 128 个,即允许有 128 个并发的连接。如果网络带宽足够,并且用户数很多,则可以设置更多。

(4) 单击“确定”按钮保存并返回,按照相同的方法可以启用或设置其他类型虚拟端口。



注意： SSTP 端口只能应用于 Windows Vista 或 Windows Server 2008 的 VPN 客户端。

3. 监控远程访问客户端

在远程访问服务器上可以查看远程访问客户端的连接属性、向远程访问客户端发送消息并断开远程访问客户端等。

(1) 单击“远程访问客户端(x)” (其中, x 代表当前连接的远程访问客户端的数量), 显示当前连接到远程访问服务器的远程客户端, 如图 16-32 所示。

(2) 选择一个远程客户端, 右击并选择快捷菜单中的“状态”选项可以查看远程客户端的输入输出字节、连接错误信息及 IP 地址等, 如图 16-33 所示。其中“连接”文本框中显示的是当前客户端使用的用户账户。

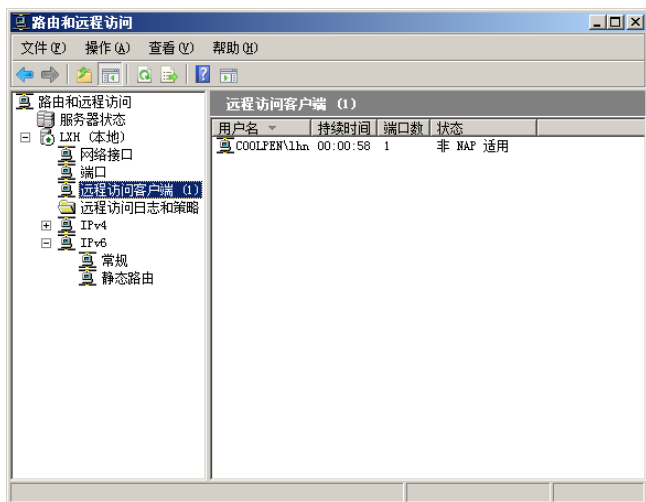


图 16-32 当前连接到远程访问服务器的远程客户端



图 16-33 客户端状态信息

(3) 单击“重置”按钮,可以复位当前客户端的状态统计信息;单击“断开”按钮,可以断开当前客户端的 VPN 连接。

4. 远程访问日志和策略

Windows Server 2008 路由和远程访问服务器的日志文件包括在 NPS 服务器日志文件中, 因此必须在 NPS 管理控制台中才能查看当前服务器的日志文件。

查看日志文件的操作步骤如下。

① 在“路由和远程访问”窗口中选择“远程访问日志和策略”选项, 显示如图 16-34 所示的“远程访问日志和策略”窗口, 在其中可设置远程访问日志记录或远程访问策略。

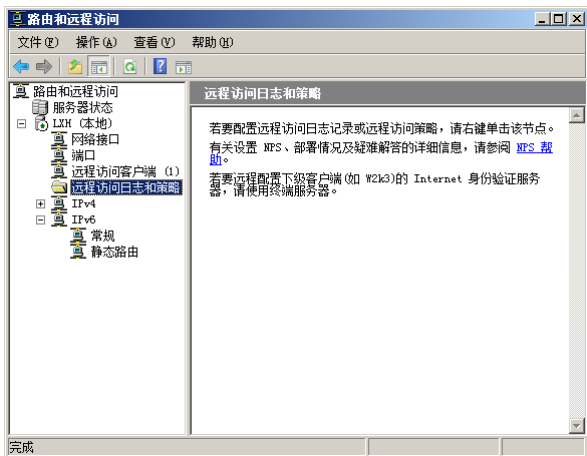


图 16-34 “远程访问日志和策略”窗口

② 右击“远程访问日志和策略”选项并选择快捷菜单中的“启用 NPS”选项, 打开如图 16-35 所示的“网络策略服务器”窗口。即使没有安装 NPS 角色, 也可以启动该窗口, 但只能查看或配置路由和远程访问服务器的日志文件。



图 16-35 “网络策略服务器”窗口

提示 如果 NPS 服务器的日志记录已经被设置为保存在 SQL 数据库中, 则需要单击“配置 SQL Server 日志记录”超级链接查看记录内容或更改基本设置, NPS 服务器日志默认保存在本地计算机。

③ 单击“配置本地文件日志记录”超级链接, 打开如图 16-36 所示的“本地文件日志记录”对话框, 在“设置”选项卡中可以设置记录的类型。

④ 打开“日志文件”选项卡，如图 16-37 所示。在其中可以设置日志文件的名称、格式及创建方式，并可在磁盘满时删除日志。

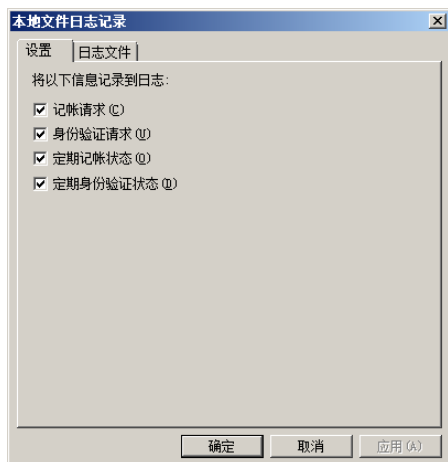


图 16-36 “本地文件日志记录”对话框

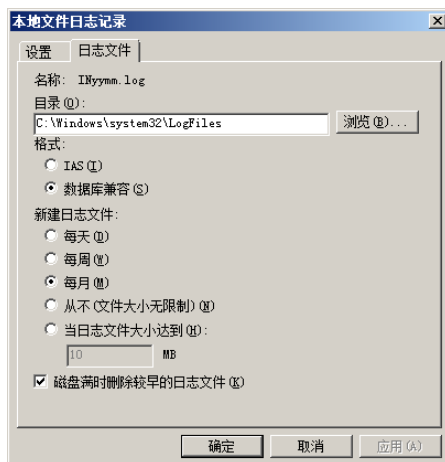


图 16-37 “日志文件”选项卡

在如图 16-38 所示的“网络策略服务器”窗口中展开“网络策略”选项即可查看原有远程访问策略，或者创建新的策略集。远程访问策略用来控制用户与远程访问服务器的连接，包括限制用户会话时间；限制只有属于某个组的用户才可以连接远程访问服务器；限制用户只能通过指定的媒介来连接，如调制解调器等；限制用户只能使用指定的验证通信协议；以及限制用户只能使用指定的信息加密方法等。

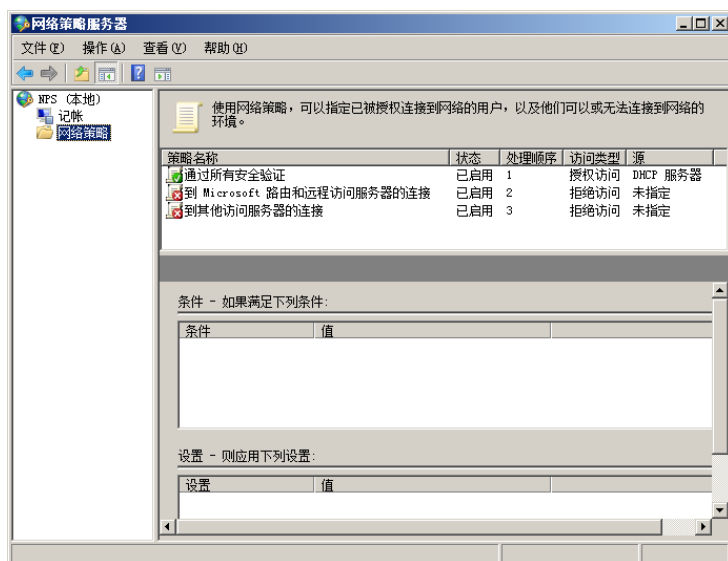


图 16-38 “网络策略服务器”窗口

默认情况下，Windows Server 2008 已经内建了两条关于路由和远程访问的策略，即“到 Microsoft 路由和远程访问服务器的连接”和“到其他访问服务器的连接”，并且已经启用。这里以创建时间限制策略为例，操作步骤如下。

① 在“网络策略服务器”窗口中右击“网络策略”选项，并选择快捷菜单中的“新建”选项。启动“新建网络策略”向导，首先显示如图 16-39 所示的“指定网络策略名称和连接类型”对话框。在“策略名称”文本框中输入策略名称，选择“网络访问服务器的类型”单选按钮，并在下拉列表框中选择“Remote Access Server (VPN-Dial up)”选项。

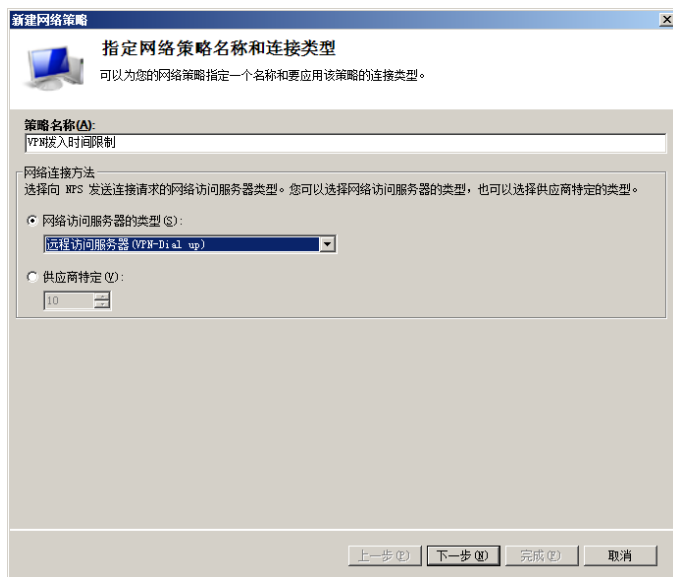


图 16-39 “指定网络策略名称和连接类型”对话框

② 单击“下一步”按钮，显示“指定条件”对话框。单击“添加”按钮，显示如图 16-40 所示的“选择条件”对话框，选择“日期和时间限制”选项。

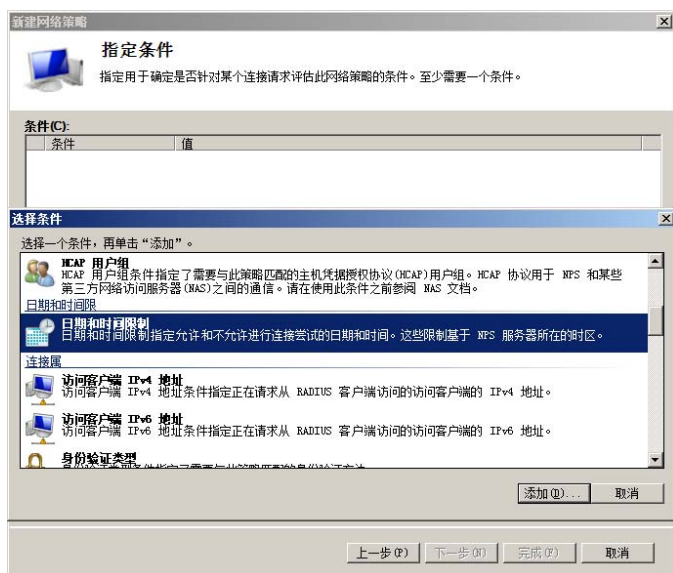


图 16-40 “选择条件”对话框

③ 单击“添加”按钮，显示如图 16-41 所示的“日期和时间限制”对话框。选择指定日期和时间范围，然后选择“允许”单选按钮即可。

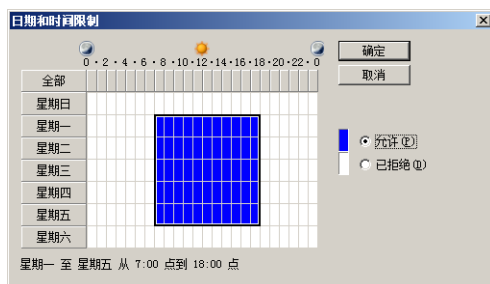


图 16-41 “日期和时间限制”对话框

④ 单击“确定”按钮，返回“指定条件”对话框。其中显示已添加的条件，如图 16-42 所示。继续单击“添加”按钮，可以添加其他限制条件，如用户账户、工作组及客户端 IP 地址等。



图 16-42 已添加的条件

⑤ 单击“下一步”按钮，显示如图 16-43 所示的“指定访问权限”对话框。在其中可以指定当连接请求符合上述条件设置时，允许用户访问还是拒绝。默认选择“已授予访问权限”单选按钮，即当客户端符合策略条件时允许访问。

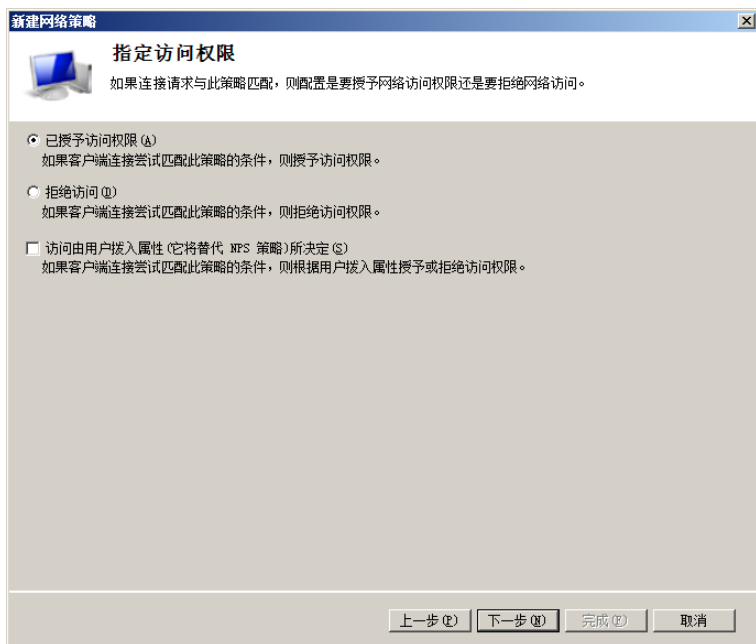


图 16-43 “指定访问权限”对话框

⑥ 单击“下一步”按钮，显示如图 16-44 所示的“配置身份验证方法”对话框，在其中配置连接请求需要与此策略匹配的身份验证方法。由于此处对 VPN 拨入连接进行限制，所以通常无需身份验证，选择“允许客户端连接而不需要协商身份验证方法”复选框即可。



图 16-44 “配置身份验证方法”对话框

⑦ 单击“下一步”按钮，显示如图 16-45 所示的“配置约束”对话框，在其中可以设置策略的附加参数。

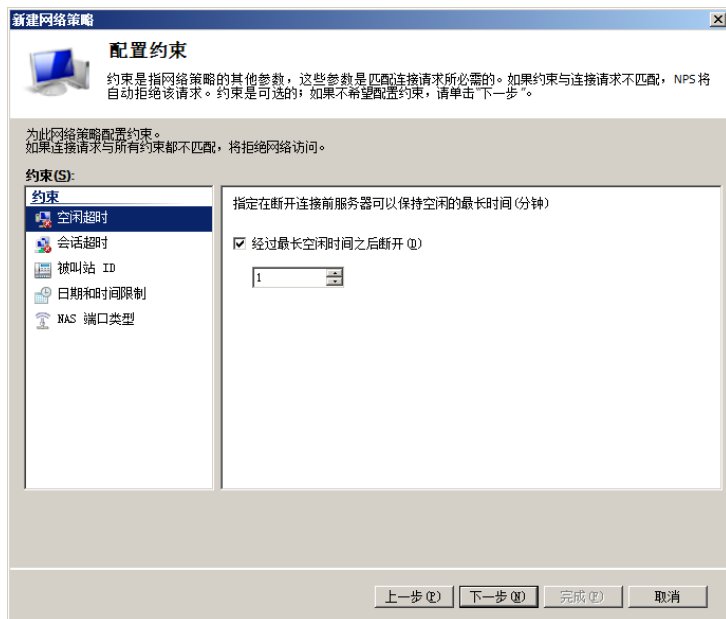


图 16-45 “配置约束”对话框

⑧ 单击“下一步”按钮，显示如图 16-46 所示的“配置设置”对话框。在其中可以设置当请求连接符合策略的所有条件和约束条件时，NPS 将应用的设置。默认为授予用户访问权限，即不应用任何设置。

⑨ 单击“下一步”按钮，显示如图 16-47 所示的“正在完成新建网络策略”对话框，其中显示前面所做的设置。

⑩ 单击“完成”按钮，退出新建网络策略向导，新配置的策略即可添加到列表框中。按照相同的操作，可以添加多条自定义网络策略。



图 16-46 “配置设置”对话框

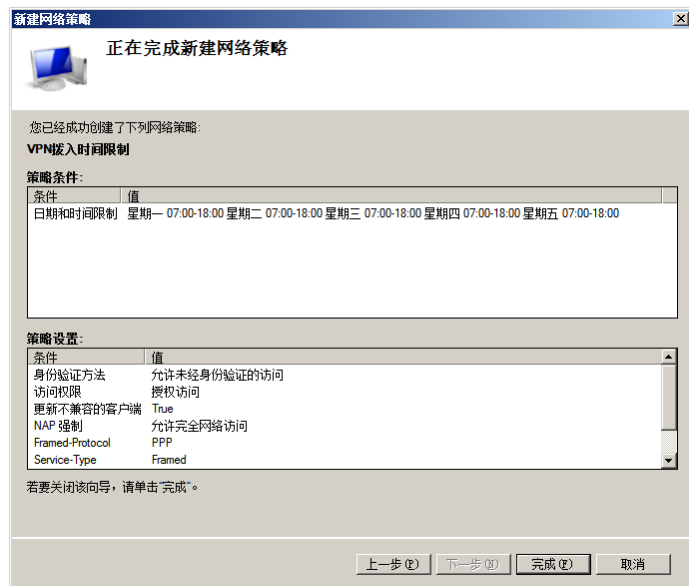


图 16-47 “正在完成新建网络策略”对话框

16.2.4 配置远程访问服务客户端

连接远程访问服务器可使用拨号或 VPN 方式，VPN 方式比拨号方式传输速率高、简便易行并且费用低廉。客户端只需接入 Internet，即可以利用 VPN 直接拨入，并且很容易达到数百 KB，甚至数 MB 的带宽。下面以 Windows Vista 为例进行介绍。

① 在 Windows Vista 系统中打开“网络和共享中心”窗口，单击“设置连接或网络”超级链接。打开如图 16-48 所示的“选择一个连接选项”对话框，选择“连接到工作区”选项。

② 单击“下一步”按钮，显示如图 16-49 所示的“您想如何连接？”对话框，在其中选择建立 VPN 连接的方式。

③ 单击“使用我的 Internet 连接 (VPN)”选项，显示如图 16-50 所示的“输入要连接的 Internet 地址”对话框。在“Internet 地址”文本框中输入 VPN 服务器的域名或公网 IP 地址，既可以是 IPv4 地址，也可以是 IPv6 地址。在“目标名称”文本框中输入 VPN 连接时显示的名称。

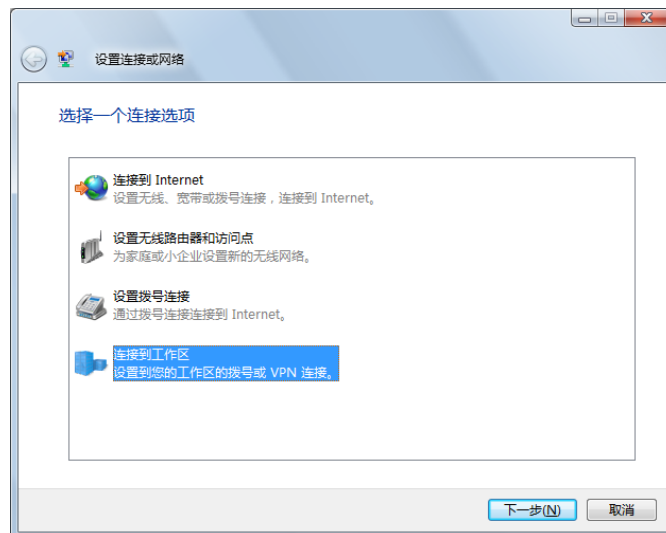


图 16-48 “选择一个连接选项”对话框



图 16-49 “您想如何连接”对话框

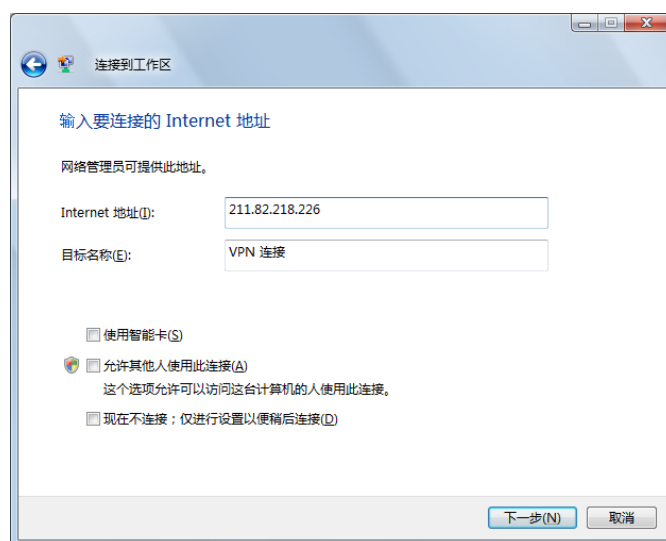


图 16-50 “输入要连接的 Internet 地址”对话框

提示 智能卡包含用户账户的重要信息,使用时将个人专用智能卡插入计算机的读卡器即可。
使用智能卡可以提供比密码更高的安全级别,当然成本也较高。

④ 单击“下一步”按钮,显示如图 16-51 所示的“输入您的用户名和密码”对话框。分别在“用户名”和“密码”文本框中输入 VPN 服务器上指定的用于 VPN 拨叫的用户账户和密码。如果 VPN 服务器指定的是域用户账户,还需要在“域”文本框中输入域名。

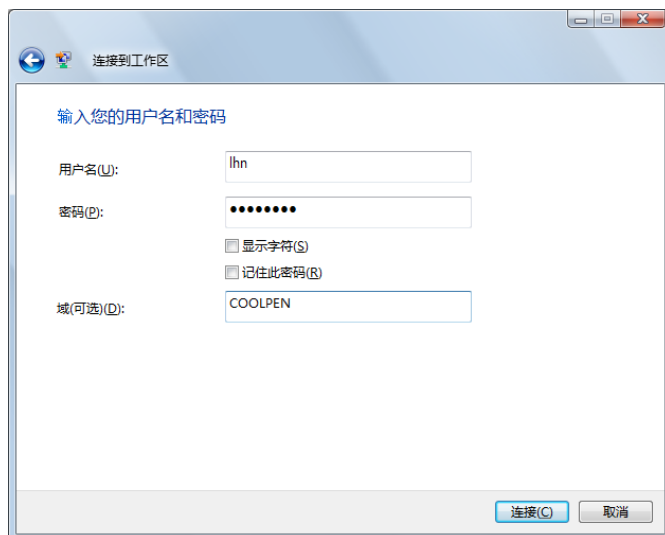


图 16-51 “输入您的用户名和密码”对话框

⑤ 单击“连接”按钮,即可尝试连接到远程 VPN 服务器。当连接成功并验证身份以后,显示如图 16-52 所示的“您已经连接”对话框,提示已经连接成功。

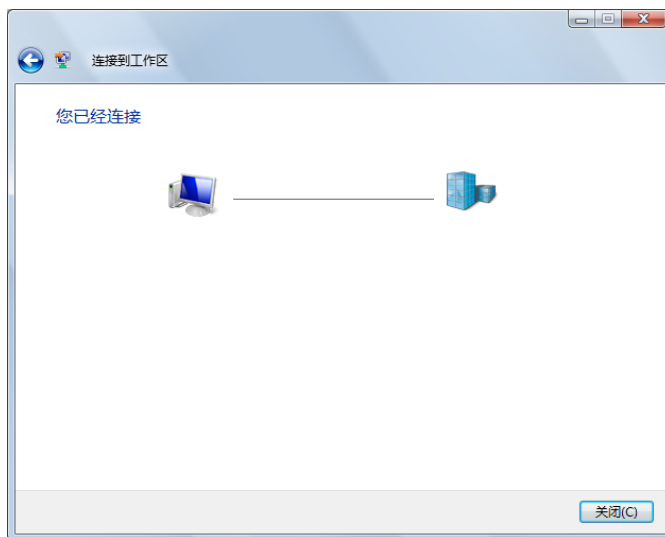


图 16-52 “您已经连接”对话框

⑥ 单击“关闭”按钮,此时即可像在本地一样使用网络中的各种资源。

注意：

当使用 VPN 连接到远程网络以后,如同位于局域网一样,在浏览网页及运行各种应用程序时都是使用该远程网络的 Internet 接入的。



如果以后需要使用 VPN 连接远程网络时,可在“网络和共享中心”窗口中单击“管理网络连接”链接。在“网络连接”窗口中双击所创建的 VPN 连接,显示如图 16-53 所示的“连接 VPN 连接”对话框,单击“连接”按钮即可连接。而右击 VPN 连接并选择快捷菜单中的“断开”选项,则可断开 VPN 连接。



图 16-53 “连接 VPN 连接”对话框

16.3 配置 NPS 策略

NPS 即网络访问策略,其中包含 4 个部分的内容,分别为网络健康验证器、更新服务器组、健康策略和网络策略,可用其完成对加入到公司网络的计算机的验证、隔离、补救及健康策略审核等。

16.3.1 配置网络健康验证器

网络健康验证器用来评估计算机运行状态需要执行的检查,并设置检查列表。根据设置的策略检测连接到网络中的计算机哪些是安全的,哪些是不安全的。例如,防火墙关闭及没有安装杀毒软件为不安全的。

① 单击“开始”→“管理工具”→“网络策略服务器”选项,打开如图 16-54 所示的“网络策略服务器”窗口。



图 16-54 “网络策略服务器”窗口

② 展开“NPS（本地）”→“网络访问保护”→“系统健康验证器”选项，如图 16-55 所示。

③ 右击“Windows 安全健康验证程序”选项，在快捷菜单中选择“属性”选项，显示如图 16-56 所示的“Windows 安全健康验证程序 属性”对话框。

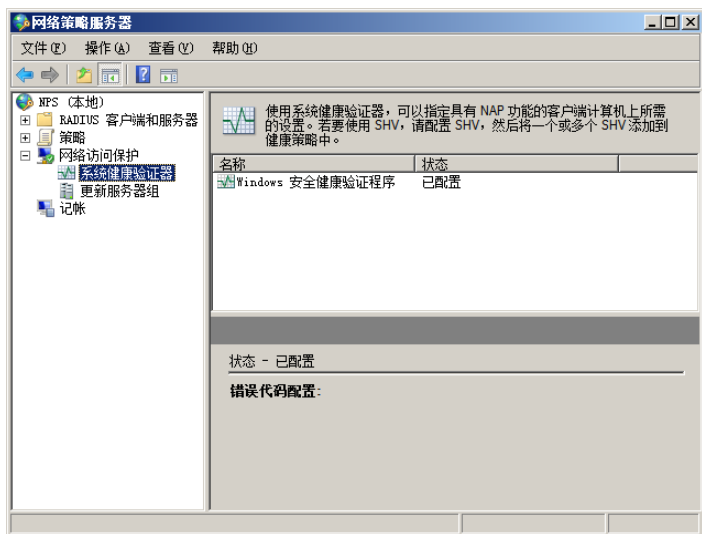


图 16-55 展开“NPS（本地）”→“网络访问保护”→“系统健康验证器”选项

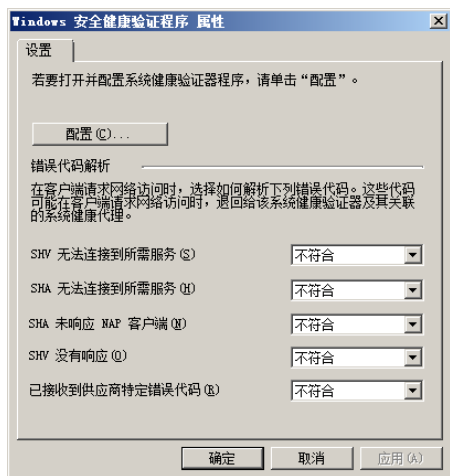


图 16-56 “Windows 安全健康验证程序 属性”对话框

④ 单击“配置”按钮，显示如图 16-57 所示的“Windows 安全健康验证程序”对话框。网络管理员应根据需要选择验证条件，如果客户端使用 Windows Vista 系统，则在“Windows Vista”选项卡中配置。

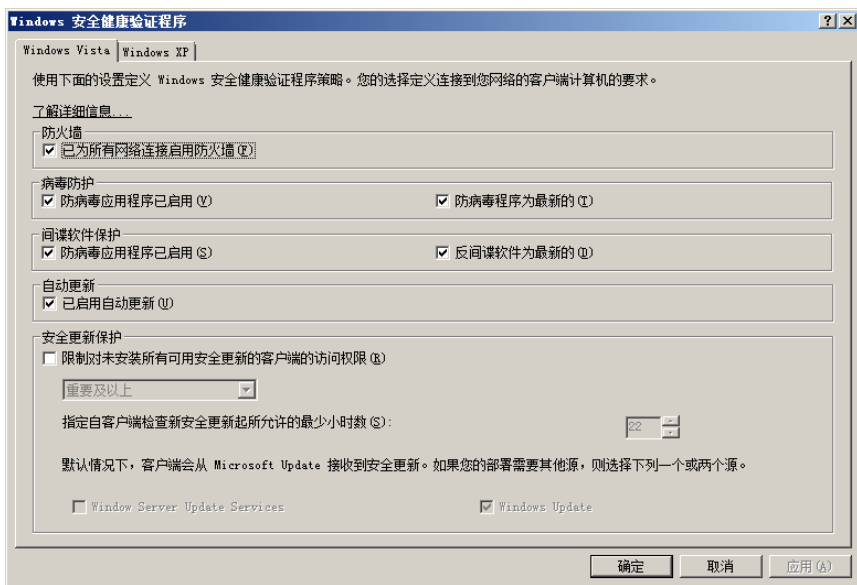


图 16-57 “Windows 安全健康验证程序”对话框

如果客户端计算机使用的是 Windows XP 系统，则在如图 16-58 所示的“Windows XP”选项卡中配置。

⑤ 单击“确定”按钮，完成 Windows 安全健康验证程序的配置。

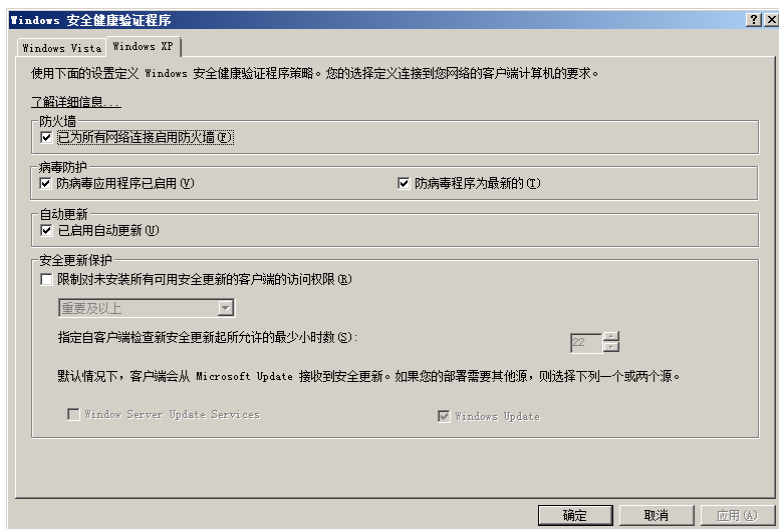


图 16-58 “Windows XP”选项卡

16.3.2 配置更新服务器组

更新服务器组允许网络管理员设置状态不良的计算机可以访问的系统（例如 WSUS 补丁服务器），通过访问定义的系统，状态不良的计算机将恢复到正常状态。在设置的过程中，注意目标服务器的 IP 地址和 DNS 域名解析要一致。

(1) 打开“网络策略服务器”窗口，展开“NPS（本地）”→“网络访问保护”→“系统健康验证器”选项，显示如图 16-59 所示的“网络策略服务器”窗口。

(2) 右击“更新服务器组”选项，在快捷菜单中选择“新建”选项，显示如图 16-60 所示的“新建更新服务器组”对话框。

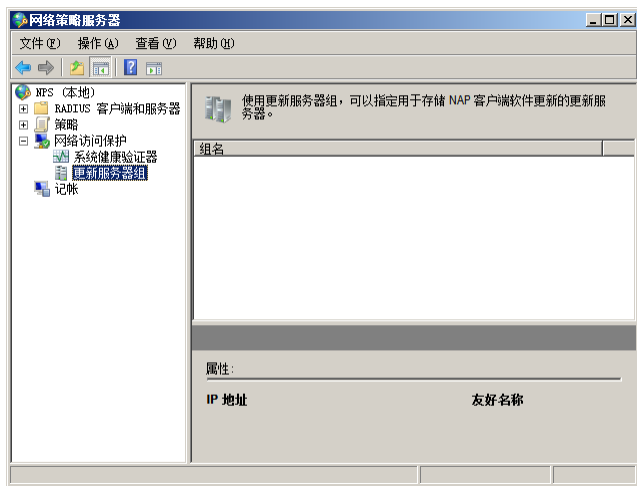


图 16-59 “网络策略服务器”窗口

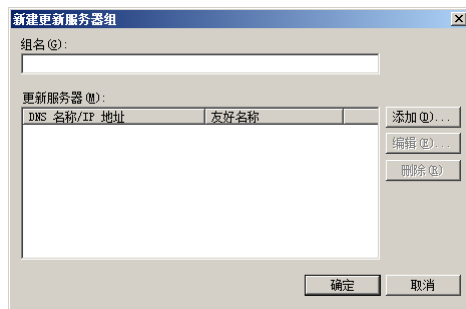


图 16-60 “新建更新服务器组”对话框

(3) 在“组名”文本框中输入服务器组的名称，单击“添加”按钮，显示如图 16-61 所示的“添加新服务器”对话框。在其中添加当客户端验证不能通过时，需要处理或者暂时访问的目标服务器。在“友好名称”文本框中输入目标服务器的标识名称，在“IP 地址或 DNS 名称”文本框中输入目标服务器的 IP 地址或 DNS 名称。单击“解析”按钮，添加解析成功的 IP 地址或 DNS 名称到“IP 地址”列表框中。

(4) 单击“确定”按钮，添加成功目标服务器，如图 16-62 所示。

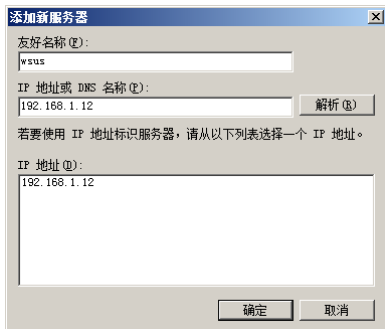


图 16-61 “添加新服务器”对话框

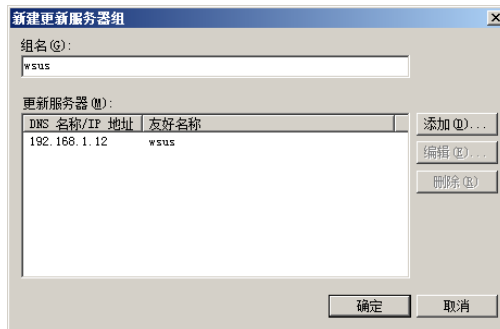


图 16-62 添加成功目标服务

(5) 单击“确定”按钮，更新服务器设置完成，如图 16-63 所示。

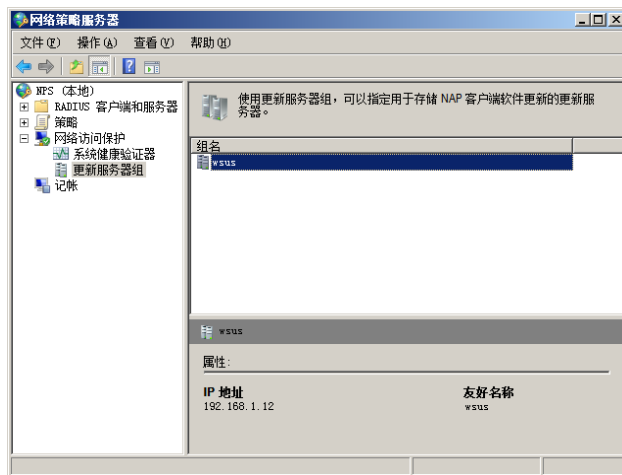


图 16-63 更新服务器设置完成

16.3.3 配置健康策略

健康策略用于创建客户端计算机是否健康的标准，建议创建两个策略，一是安全计算机的策略；二是不安全计算机的策略。如果网络健康验证器验证的计算机是安全的，则归类到安全计算机的策略中；如果网络健康验证器验证计算机是不安全的，将归类到不安全计算机的策略中。

(1) 打开如图 16-64 所示的“网络策略服务器”窗口，展开“NPS (本地)”→“策略”→“健康策略”选项。

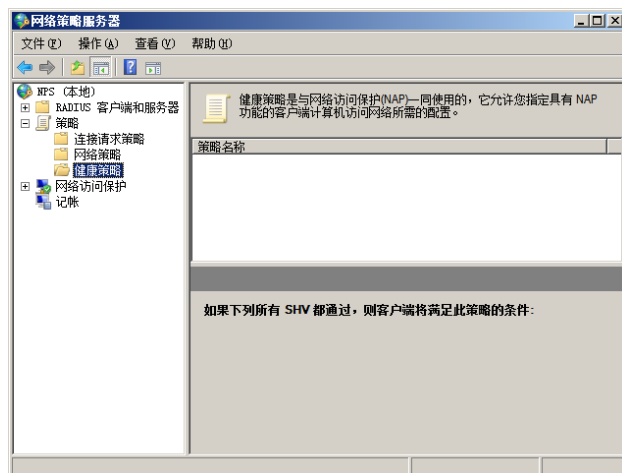


图 16-64 “网络策略服务器”窗口

(2) 右击“健康策略”选项并从快捷菜单中选择“新建”选项，显示如图 16-65 所示的“新建健康策略”对话框，在其中创建“通过所有安全健康检查”策略。

设置如下选项。

策略名称：输入策略名称；

客户 SHV 检查：选择“客户端通过了所有 SHV 检查”选项；

此健康策略中使用的 SHV：选中“Windows 安全健康验证程序”复选框。

(3) 单击“确定”按钮，创建完成新策略。按照同样方法创建“没有通过安全健康检查”策略，如图 16-66 所示。

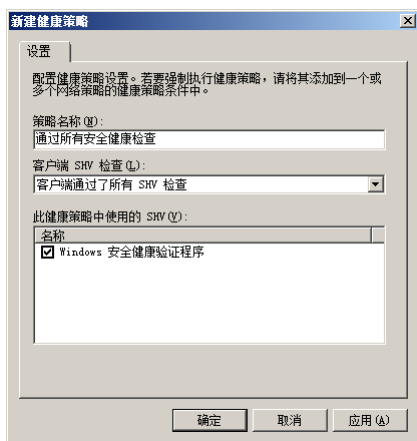


图 16-65 “新建健康策略”对话框

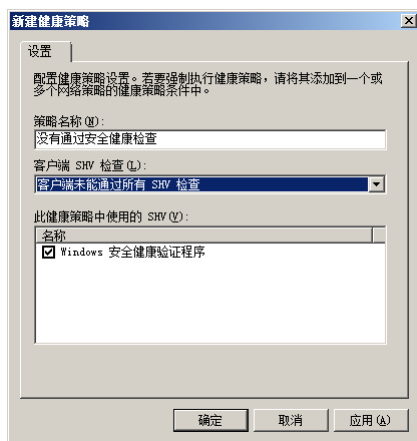


图 16-66 创建“没有通过安全健康检查”策略

(4) 创建完成后，所有的策略显示在“健康策略”窗口中，如图 16-67 所示。

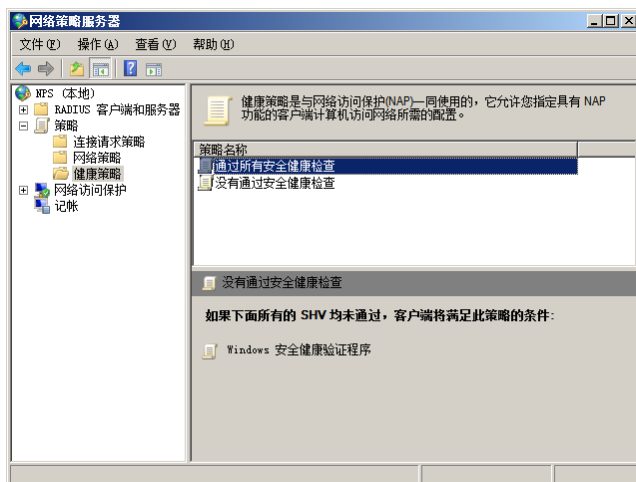


图 16-67 所有的策略

16.3.4 配置网络策略

网络策略定义处理逻辑规则，根据计算机运行状况确定如何对其进行处理。网络健康验证器、更新服务器组，以及健康处理通过网络策略组合在一起。网络策略由管理员定义，用于指导 NPS 如何根据计算机的运行状态处理计算机。NPS 会从上到下评估这些策略，一旦计算机与策略规则相符，处理将立即停止。

本节示例将创建两条策略，分别为“通过所有安全验证”和“没有通过网络安全检查”策略。

(1) “通过所有安全验证”策略：

规定通过所有“安全中心”检查的计算机可以获得不受限制的网络访问权限，即当计算机经过运

行状况评估并通过所有检查时，NPS 会指示 DHCP 服务器为该计算机提供一个作用域选项为“正常”的 IP 租约。此策略通常应该列在处理顺序的首位，因为大多数计算机在接受这项检查时应该都是符合规则的，列在首位可减少 NPS 的处理工作量和时间。

(2) “没有通过网络安全检查”策略：

对应任何未通过一项或多项 SHV 检查的计算机，如果有计算机与此策略相符，则 NPS 会指示 DHCP 服务器为该客户端提供一个具有特殊 NAP 受限作用域选项的 IP 租约，该地址仅允许违规计算机访问更新服务器组中定义的资源。

① 打开“网络策略服务器”窗口，依次展开“NPS（本地）”→“策略”→“网络策略”选项，如图 16-68 所示。

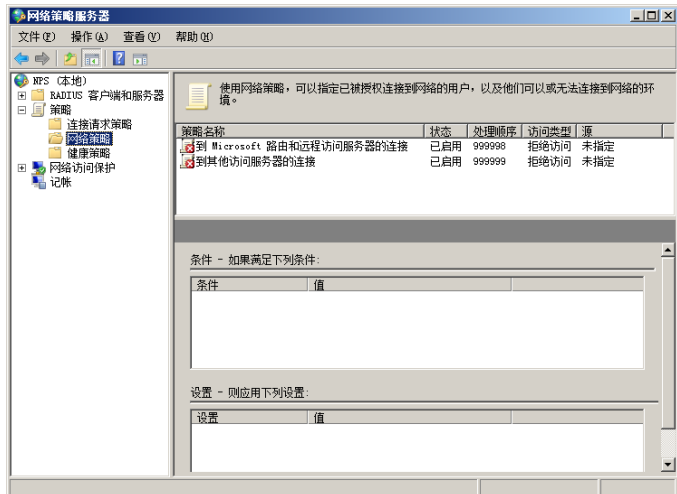


图 16-68 展开“NPS（本地）”→“策略”→“网络策略”选项

② 右击“网络策略”选项，在快捷菜单中选择“新建”选项，启动“新建网络策略”向导。显示如图 16-69 所示的“指定网络策略名称和连接类型”对话框，在“策略名称”文本框中键入策略名称，例如“通过所有安全验证”。选择“网络访问服务器的类型”单选按钮，并在下拉列表框中选择“DHCP 服务器”选项。

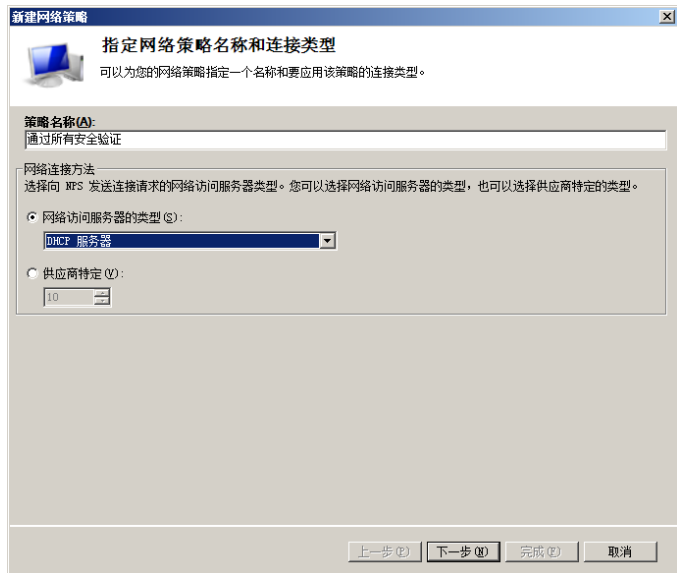


图 16-69 “指定网络策略名称和连接类型”对话框

③ 单击“下一步”按钮，显示如图 16-70 所示的“指定条件”对话框。

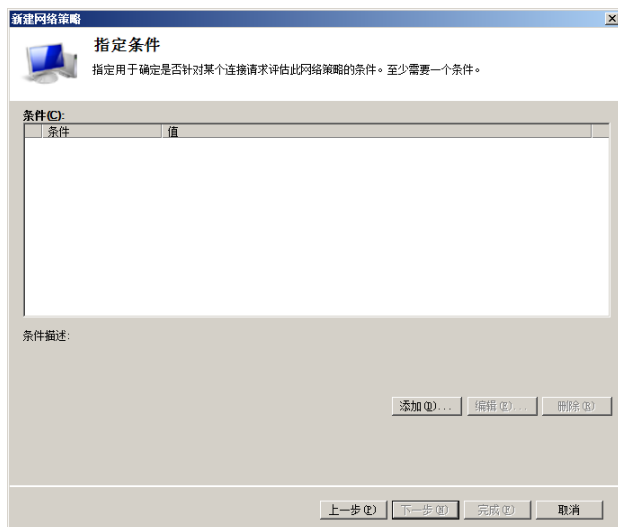


图 16-70 “指定条件”对话框

④ 单击“添加”按钮，显示如图 16-71 所示的“选择条件”对话框，在下拉列表框中选择“健康策略”选项。

⑤ 单击“添加”按钮，显示如图 16-72 所示的“健康策略”对话框，在“健康策略”下拉列表框中选择“通过所有安全健康检查”选项。

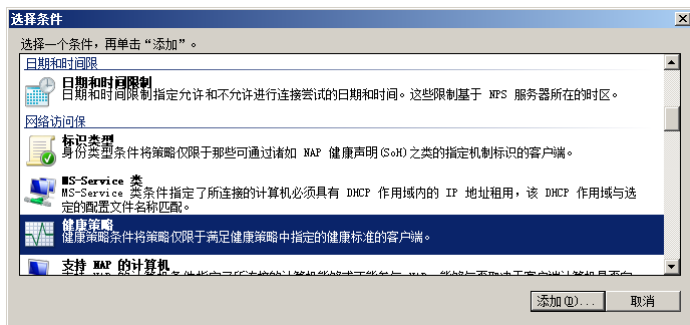


图 16-71 “选择条件”对话框

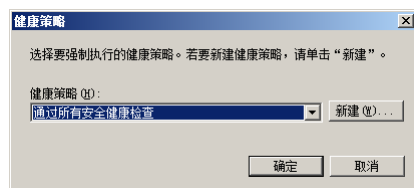


图 16-72 “健康策略”对话框

⑥ 单击“确定”按钮，关闭“健康策略”对话框并返回到“指定条件”对话框，如图 16-73 所示。

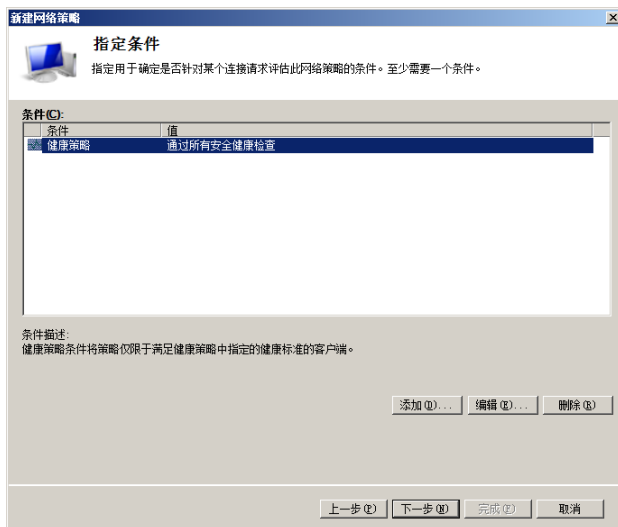


图 16-73 “指定条件”对话框

⑦ 单击“下一步”按钮，显示如图 16-74 所示的“指定访问权限”对话框。选择“已授予访问权限”单选按钮，允许通过验证的客户端访问网络。

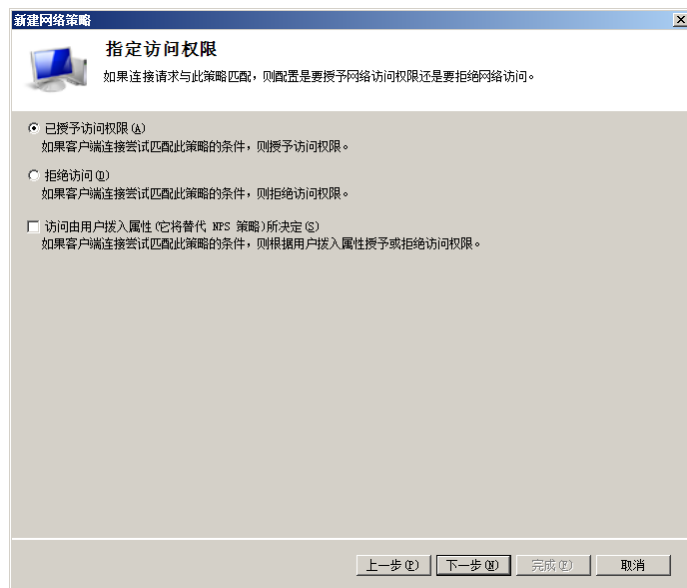


图 16-74 “指定访问权限”对话框

⑧ 单击“下一步”按钮，显示如图 16-75 所示的“配置身份验证方法”对话框，在其中选择一种或多种身份验证方法。这里使用健康程序仅对客户端进行健康验证，因此选择“仅执行计算机健康检查”单选按钮。

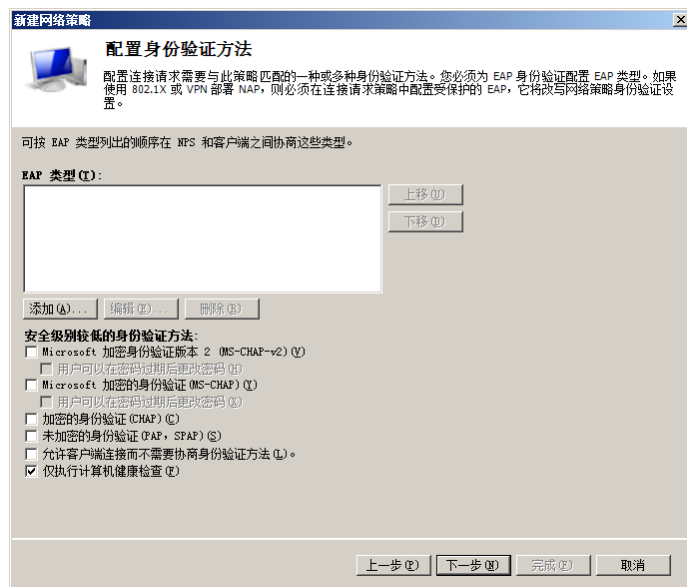


图 16-75 “配置身份验证方法”对话框

⑨ 单击“下一步”按钮，显示如图 16-76 所示的“配置约束”对话框。

⑩ 单击“下一步”按钮，显示如图 16-77 所示的“配置设置”对话框。在左窗格的“设置”下拉列表框中选择“网络访问保护”下的“NAP 强制”选项，然后选择“允许完全网络访问”单选按钮，所有通过安全计算的计算机将允许访问网络。

⑪ 单击“下一步”按钮，显示如图 16-78 所示的“正在完成新建网络策略”对话框，其中显示新建网络策略的配置信息。

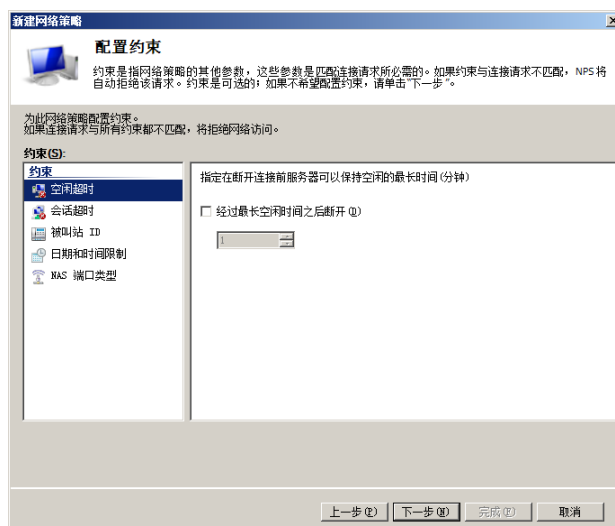


图 16-76 “配置约束”对话框



图 16-77 “配置设置”对话框

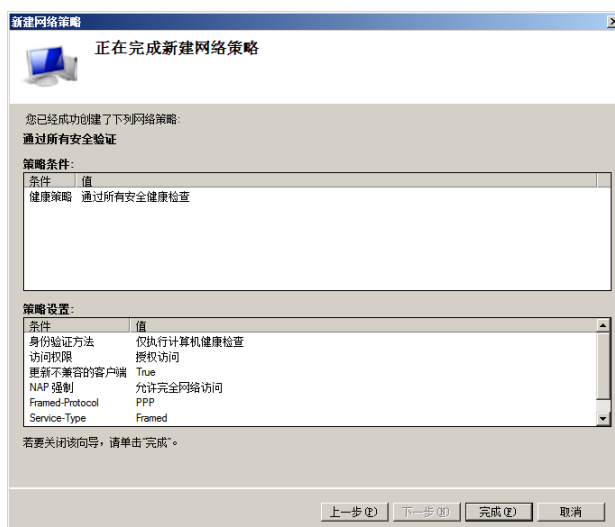


图 16-78 “正在完成新建网络策略”对话框

12 单击“完成”按钮，创建成功新策略，如图 16-79 所示。

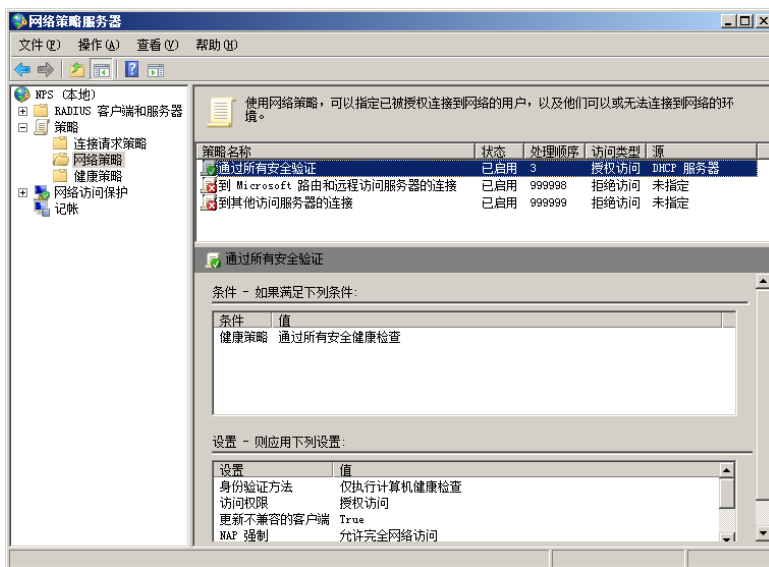


图 16-79 创建成功新策略

按照同样方法可以创建“没有通过网络安全检查”策略，在创建的过程中注意如下问题。

(1) 在如图 16-80 所示的“指定条件”对话框中添加条件时，选择“没有通过安全健康检查”策略。

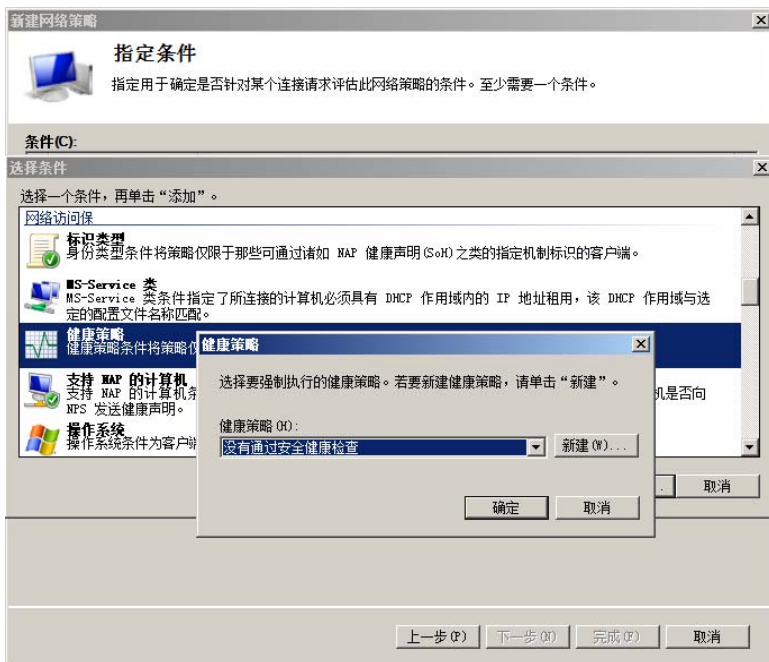


图 16-80 “指定条件”对话框

(2) 在如图 16-81 所示的“配置设置”对话框中选择“允许受限访问”单选按钮，当没有通过安全健康检查时，将不允许访问网络或者指定到目标服务器上完成必须的系统更新。

创建完成的网络策略显示在“网络策略”窗口中，如图 16-82 所示。



图 16-81 “配置设置”对话框

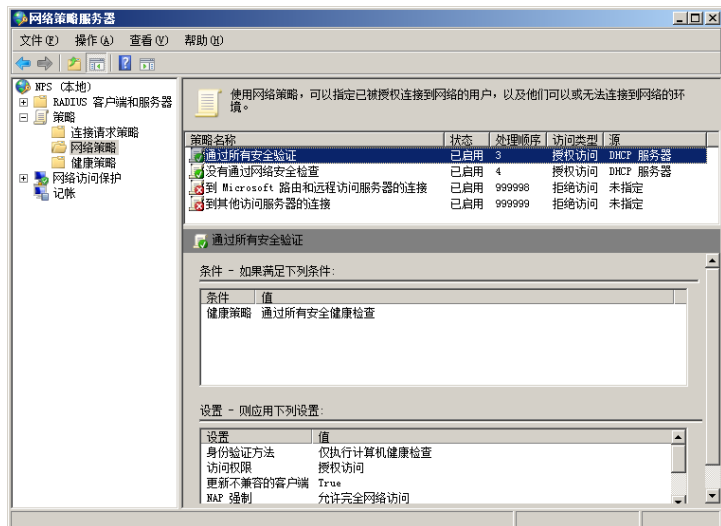


图 16-82 创建完成的网络策略

16.4 配置 NPS 客户端

当服务器配置 NPS 策略以后，还需要对客户端进行一定的配置，才能实现对客户端的网络访问保护。为了提高工作效率，通常可对域中的计算机使用组策略进行全局部署。本节，以 Windows Vista 为例说明如何以手动方式配置客户端，从而完成 NAP 保护功能。

16.4.1 启用安全中心

在本地策略中启用“启用安全中心（仅限域 PC）”策略，默认未启用。在 Active Directory 环境中，建议使用组策略的方式集中部署。

① 打开“开始”菜单，在“开始搜索”文本框中输入“gpedit.msc”。按回车键，打开如图 16-83 所示的“组策略对象编辑器”窗口。展开“本地计算机策略”→“计算机配置”→“管理模板”→“Windows 组件”→“安全中心”选项。

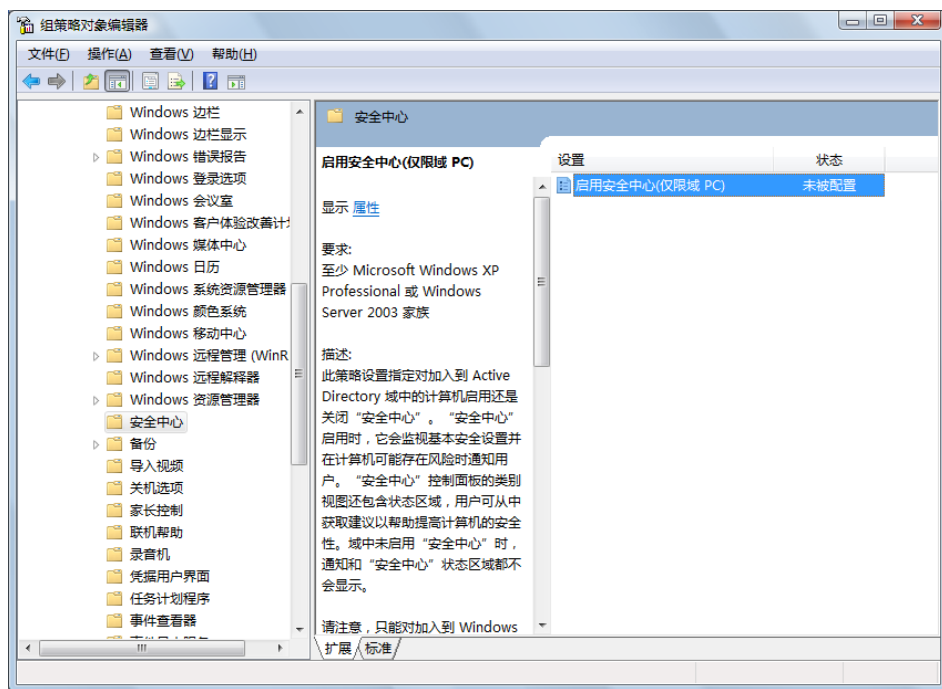


图 16-83 “组策略对象编辑器”窗口

② 右击“启用安全中心（仅限域 PC）”选项，在快捷菜单中选择“属性”选项。显示如图 16-84 所示的“启用安全中心（仅限域 PC）属性”对话框，选择“已启用”单选按钮。

③ 单击“确定”按钮，完成策略设置。

④ 打开命令提示符窗口，输入如下命令：

```
Gpupdate /force
```

按回车键，组策略更改立即生效，如图 16-85 所示。

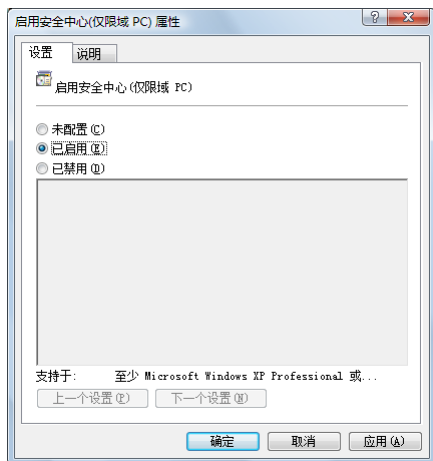


图 16-84 “启用安全中心（仅限域 PC）属性”对话框

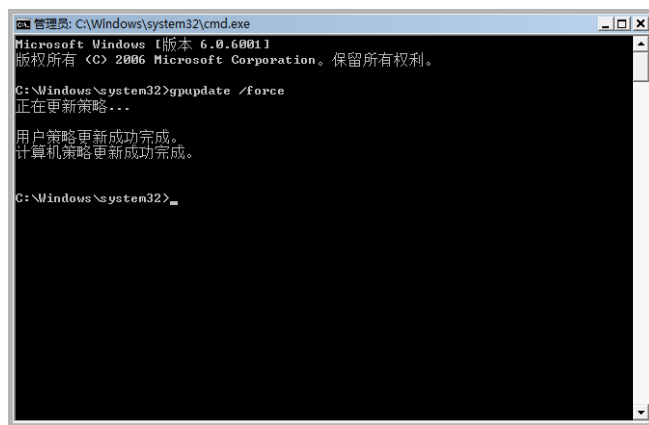


图 16-85 组策略更改立即生效

16.4.2 配置 NAP 客户端

在 Windows Vista 操作系统中，默认安装了 NAP 客户端工具。本节将在 Windows Vista 系统中启用“DHCP 隔离强制客户端”策略来强制使用 DHCP 安全保护策略。

① 打开“开始”菜单，在“开始搜索”文本框中输入“napclcfg.msc”。按回车键，显示如图 16-86 所示的“NAP 客户端配置”窗口。



图 16-86 “NAP 客户端配置”窗口

② 展开“NAP 客户端配置（本地计算机）”→“强制客户端”选项，如图 16-87 所示。默认情况下，“DHCP 隔离强制客户端”处于禁用状态。

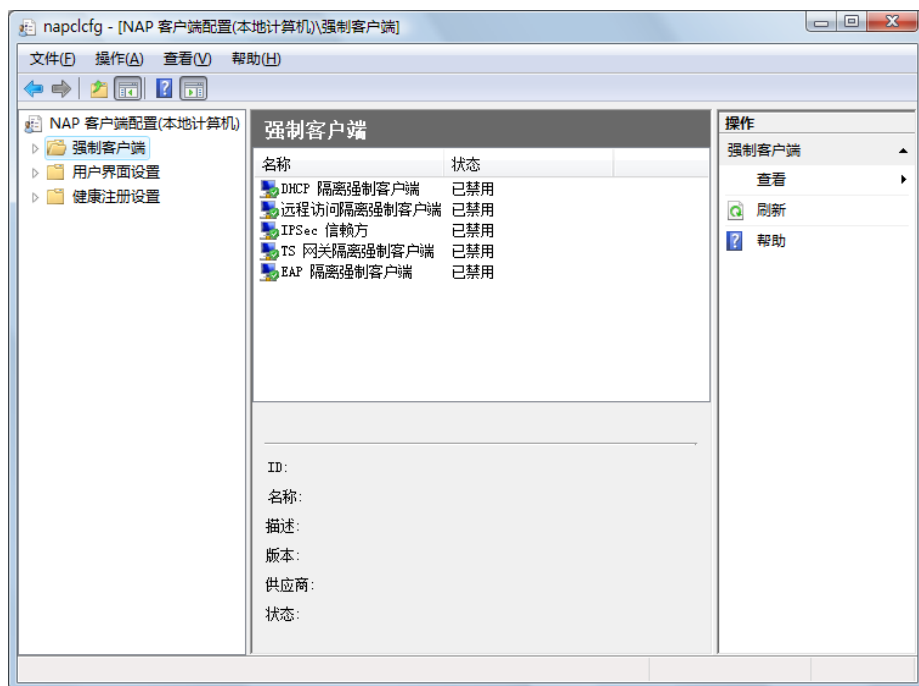


图 16-87 展开“NAP 客户端配置（本地计算机）”→“强制客户端”选项

③ 选择“DHCP 隔离强制客户端”策略，右击并在快捷菜单中选择“启用”选项。启用“DHCP 隔离强制客户端”，如图 16-88 所示。



图 16-88 启用“DHCP 隔离强制客户端”策略

16.4.3 配置 NAP 代理服务

NAP (Network Access Protection Agent) 代理服务默认情况下为禁用状态，建议将其设置为随系统自动启动。

① 单击“开始”→“控制面板”→“管理工具”→“服务”选项，显示如图 16-89 所示的“服务”窗口，在右窗格的“服务”列表框中选择“Network Access Protection Agent”服务。

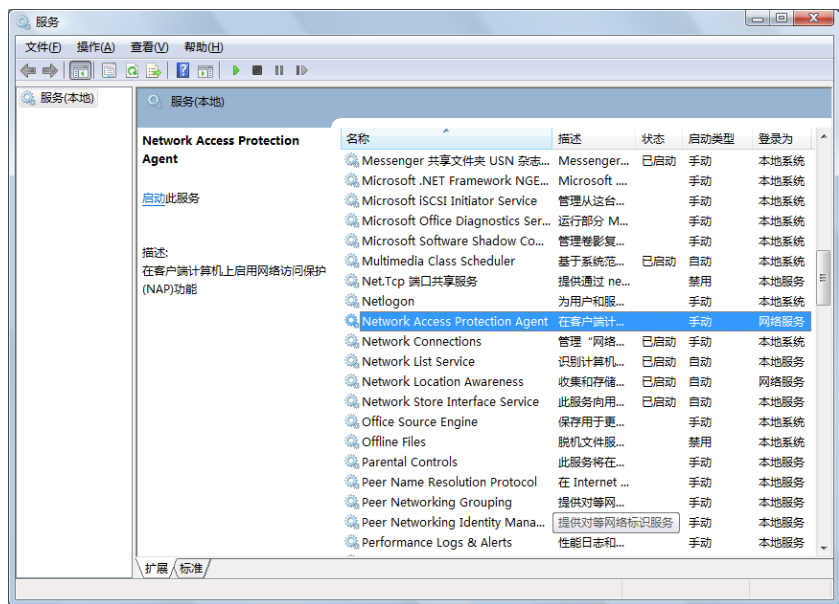


图 16-89 “服务”窗口

② 右击“Network Access Protection Agent”选项，在快捷菜单中选择“属性”选项，显示如图 16-90 所示的“Network Access Protection Agent 的属性”对话框。在“常规”选项卡的“启动类型”下拉列表框中选择“启动”选项，使客户端在启动时自动运行 NAP 代理服务。

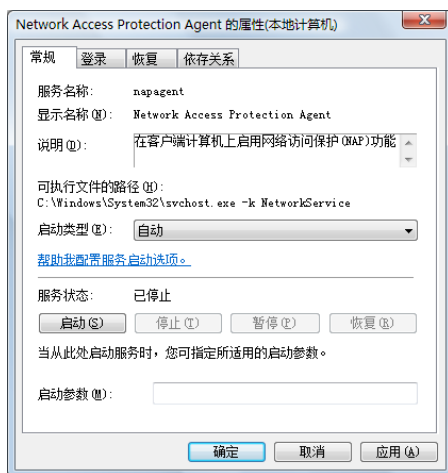


图 16-90 “Network Access Protection Agent 的属性”对话框

- ③ 单击“确定”按钮，完成 NAP 代理服务的设置。

16.5 Windows Server 2000/2003 的配置差异

Windows Server 2003 中只集成了“路由和远程访问”功能，可以配置为 VPN 服务器，为远程用户提供 VPN 接入。不过没有集成 NAP 服务，因此无法通过 NAP 策略来限制客户端。

第 17 章 AD RMS 服务

文件安全是网络领域中最重要课题之一，安全的威胁通常来自 Internet 和局域网内部两个方面。“日防夜防，家贼难防”。来自企业内部的攻击往往是最致命的，微软公司的 RMS（Rights Management Services，权限管理服务）正是在这种环境下应运而生的。它通过数字证书和用户身份验证技术对各种 Office 文档的访问权限加以限制，可以有效防止内部用户通过各种途径擅自泄露机密文档内容，从而确保了数据文件访问的安全性。

17.1 AD RMS 概述

对于 RMS，很多用户并不陌生，并且可能已经应用到实际环境中。AD RMS 是在 RMS 基础上进行了一些改进，功能更加强大。通过与 Active Directory 及其联合身份验证等服务的配合应用，不仅仍然具备原有的针对 Office 文档的各种权限保护，而且新增了通过 MMC 控制台管理 AD RMS 的功能，应用更加方便。

17.1.1 AD RMS 的新特性

AD RMS 与 RMS 相比具有如下新特性。

（1）管理界面更加友好：在 RMS 1.0 中唯一的管理界面就是 Web，而 AD RMS 则改用 MMC 嵌入式管理单元，操作更加方便。

（2）自动启用服务器授权凭证：在 AD RMS 中，根群集的服务器授权凭证（Server Licensor Certificate，SLC）可以自动启用，无须手动操作。

（3）与 Active Directory 联合身份验证服务（AD FS）配合使用：AD FS 是 Windows Server 2008 的一项新功能，可以提供简单且安全的身份验证。AD RMS 与 AD FS 配合使用，可以允许企业之间共同使用一方的 AD RMS 群集，并且通过 AD FS（使用 HTTPS 协议）识别和验证自己域中的用户账户。

17.1.2 AD RMS 的相关组件

AD RMS 仍然基于服务器/客户端的结构，其主要组件包括支持 AD RMS 的应用程序、AD RMS 客户端和 AD RMS 服务器端三，三者缺一不可。只有支持 AD RMS 的应用程序才能生成被保护的文档；AD RMS 客户端是安装在客户端上，与支持 AD RMS 的应用程序交互；AD RMS 服务器负责为信任实体颁发证书、授权服务器，并为使用 AD RMS 保护的文档授权。

使用权限账户证书可以将用户账户和具体的一台设备关联起来，即每个不同的账户在同一台计算机上存在唯一的权限证书，或同一账户在不同的计算机上的权限证书也不相同。虽然在不同用户的权限账户证书不同，但是其中所包含的密钥却是相同的。该权限账户证书是由企业中的第 1 台 AD RMS 服务器所颁发的，即在任何计算机上的用户的密钥对相同，当用户向 AD RMS 许可服务器请求许可时需要使用权限账户证书。

权限账户证书的生成过程如下。

（1）当用户第 1 次使用由 AD RMS 加密的文档时，需要以域用户的身份向 AD RMS 证书服务器发送请求来获取权限账户证书。

（2）服务器会在服务器数据库中所存的信息查询，如果该用户已经存在密钥对，则会应用已有的

密钥；否则会为该用户生成一个密钥对。

(3) 服务器会将该用户的密钥对中的私钥用该证书服务器的私钥进行加密。

(4) 服务器将用户密钥对中的公钥和加密后的私钥放到权限账户证书中。

(5) 权限账户证书会被 AD RMS 服务器用私钥进行数字签署，这样就能确定该权限账户证书由 AD RMS 证书服务器所发放的，并且未被篡改。

(6) AD RMS 服务器将权限账户证书发送给用户。

(7) 服务器将用户的密钥对存储到 AD RMS 的数据库中，该权限账户证书就是以后该用户进行申请各种使用许可的证书。

►► 17.1.3 AD RMS 的实现原理

1. 服务的发现

服务的发现实际上是 RMS 客户端发现 AD RMS 服务器的一个过程，该过程可以通过两种方法来实现，一是通过活动目录中的服务连接点（SCP），找到企业中的证书服务器的位置；二是通过注册表。

找到 AD RMS 服务可以激活 RMS 客户端，因为如果要使用该 RMS 客户端，则必须在第 1 次使用时到 AD RMS 服务器激活该 RMS 客户端，可以从 AD RMS 服务器上获取权限管理账户证书等信息。

2. 文档的在线发布过程

由 RMS 客户端在线向授权服务器发送请求，发布过程如下。

(1) 由密码箱生成对称密钥作为内容密钥。

(2) 内容密钥会被授权服务器的公钥加密，目的是通过网络将其发送给授权服务器。然后授权服务器能够用自己的私钥将这个内容解出，而在传送的过程中不会被他人截获后获取内容密钥。

(3) 加密的内容密钥和权限被发送给请求发布许可的授权服务器。

(4) 授权服务器使用其私钥解开加密的内容密钥。

(5) 授权服务器使用其公钥加密内容密钥和使用权限。

(6) 加密后的密钥和使用权限被添加到发布许可中。

(7) 授权服务器使用私钥签署发布许可。

(8) 发布许可返回给申请的客户端。

(9) 支持 AD RMS 的应用程序将发布许可合并到受保护的文档中。

3. 文档的离线发布过程

如果用户所使用的是笔记本电脑等移动办公等的计算机设备，有可能在自己的家中不能够连接到公司的 AD RMS 服务器。为访问使用由 AD RMS 创建的文档，需要一个客户端许可证书（CLC）。保护过程如下：

(1) 由密码箱生成对称密钥作为内容密钥。

(2) 客户端从客户端许可证书中取出授权服务器的公钥。

(3) 客户端使用服务器的公钥加密内容密钥，加密的内容密钥只能由服务器的私钥所解密。

(4) 客户端使用客户端许可证书的公钥对内容密钥再进行一次加密，从而再次获得一个加密后的对称密钥。需要注意的是，在离线和在线发布不同是离线发布过程中对内容进行了两次加密。

(5) 两个加密后的对称密钥同时被放到发布许可中。

(6) 客户端使用权限账户证书中的私钥解密客户端许可证书中的私钥。

(7) 客户端使用 CLC 的私钥签署发布许可。

(8) 支持 AD RMS 的应用程序将发布许可合到受保护的文档中。

4. 受保护文档的使用过程

使用受保护文档的具体过程如下。

- (1) 客户端将权限账户证书和文档的发布许可发送到颁发发布许可的授权服务器。
- (2) 授权服务器使用其私钥解出发布许可中的内容密钥。
- (3) 授权服务器使用权限账户证书中用户的公钥加密内容密钥。
- (4) 把加密的内容密钥和用户的使用权限添加到使用许可中。
- (5) 授权服务器使用其私钥签署使用许可。
- (6) 作为响应, 将该使用许可发送给客户端。
- (7) 密码箱使用计算机的私钥解密保存在权限账户证书中和用户私钥。
- (8) 密码箱使用用户的私钥解密内容密钥。
- (9) 密码箱使用内容密钥解密被加密的受保护内容。

提示

使用服务器的公钥所加密的内容只能由服务器的私钥来解开。

►► 17.1.4 AD RMS 服务器的软件需求

AD RMS 服务器的软件需求如下。

- (1) 必须是域控制器、额外的域控制器或域成员服务器。
- (2) 安装 IIS 服务和 ASP.Net 组件。
- (3) 安装 MSMQ (消息队列) 服务。
- (4) 如果要创建 AD RMS 服务器群集, 需要安装 SQL Server 数据库服务器或 MSDE 数据库 (建议选择 SQL Server); 否则可以直接使用 AD RMS 自带的本地数据库。

提示



AD RMS 服务器软件需要提前安装的 Windows 组件, 在安装过程中可以自动安装, 用户不必一一手动准备。

17.2 AD RMS 服务器的安装和配置

Windows Server 2008 中的 AD RMS 与 RMS 最大的区别就在于, 它不再是一个独立服务插件, 已经成为 Windows 的一项内建功能, 并且包含了某些升级功能。无须下载任何安装包, 直接在管理服务器窗口中启动安装向导即可轻松安装。

►► 17.2.1 准备工作

为了确保安装过程可以顺利进行, 开始之前应做好如下准备工作:

- (1) 将计算机加入到域, 或者提升为域的辅助域控制器, 或者子域。
- (2) 使用具有域用户账户登录, 但不能使用 Administrator 账户登录。
- (3) 选择数据库。如果要使用独立数据库, 需安装 SQL Server; 否则可使用 AD RMS 的自带数据库。
- (4) 安装之前, 确认 <http://uddi.microsoft.com> 和 <https://uddi.microsoft.com> 在 Internet Explorer 中被添加至“受信任的站点”或“本地 Internet”。

►► 17.2.2 安装 AD RMS 根服务器

AD RMS 服务并不是 Windows Server 2008 系统默认安装的组件, 需要用户手动添加。安装向导如果检测到有完成的准备工作, 显示提示信息并给出解决方案, 通常情况下可以自动完成必要组件的安装。

- ① 使用具有域权限的用户账户登录。运行“添加角色向导”。在“选择服务器角色”对话框中,

选中“Active Directory Rights Management Services”复选框，显示如图 17-1 所示对话框，提示是否添加所需的角色服务和功能。



图 17-1 添加所需的角色服务和功能

② 单击“添加必需的角色服务”按钮，显示如图 17-2 所示的“选择服务器角色”对话框，选中“Active Directory Rights Management Services”复选框。

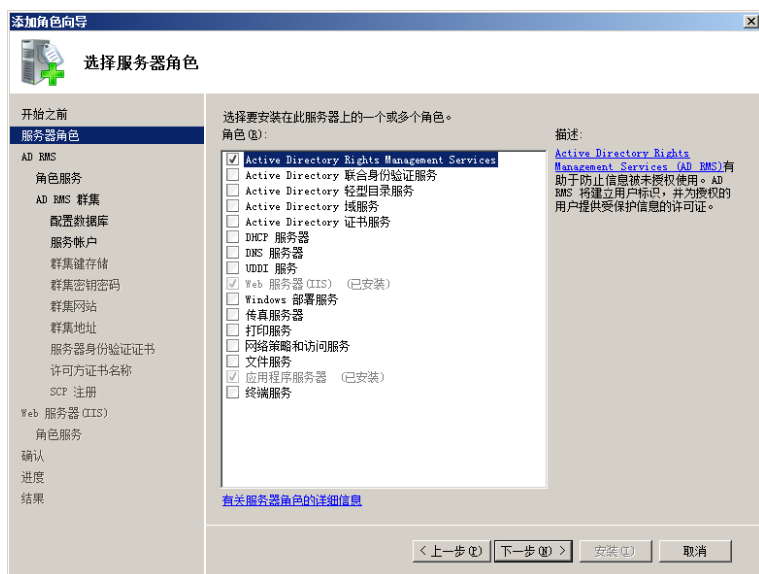


图 17-2 “选择服务器角色”对话框



提示

不能使用 Administrator 用户账户登录；否则就会显示如图 17-3 所示的警告框，提示无法安装。



图 17-3 警告框

③ 单击“下一步”按钮，显示如图 17-4 所示的“Active Directory Rights Management Services”对话框，其中简要介绍了 Active Directory 权限管理服务的作用及功能。

④ 单击“下一步”按钮，显示如图 17-5 所示的“选择角色服务”对话框。如果选中“联合身份验证支持”复选框，将同时安装 AD FS 或与当前域中已有的 AD FS 关联使用。它允许用户使用当前域和其他域之间经过联合身份验证的信任关系来建立用户标识，并提供对其他组织创建的受保护信息的访问权限。不需要联合身份验证的用户建议不要选择该复选框。



图 17-4 “Active Directory Rights Management Services” 对话框

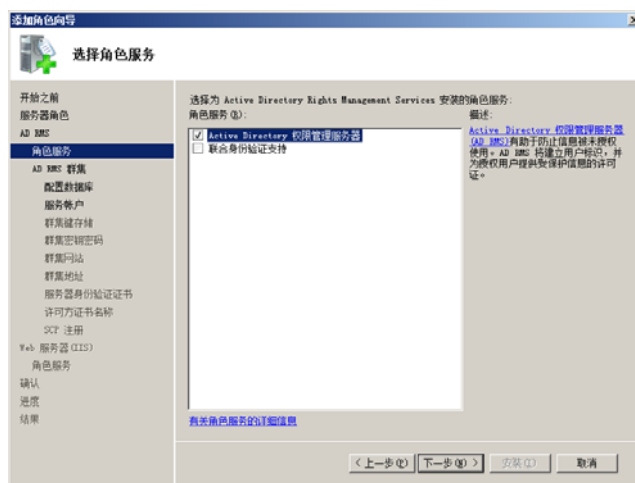


图 17-5 “选择角色服务” 对话框

⑤ 单击“下一步”按钮，显示如图 17-6 所示的“创建或加入 AD RMS 群集”对话框，系统默认选择“新建 AD RMS 群集”单选按钮。由于当前域中没有其他 AD RMS 群集可供加入，所以“加入现有 AD RMS 群集”单选按钮为灰色。安装完成后创建的第 1 台 AD RMS 服务器即为根群集，后来加入的 AD RMS 服务器为叶服务器。



图 17-6 “创建或加入 AD RMS 群集” 对话框

⑥ 单击“下一步”按钮，显示如图 17-7 所示的“选择配置数据库”对话框。如果网络中安装有 SQL Server 服务器，可选择“使用其他数据库服务器”单选按钮；如果要使用 AD RMS 自带的数据库，选择“在此服务器上使用 Windows 内部数据库”单选按钮即可。

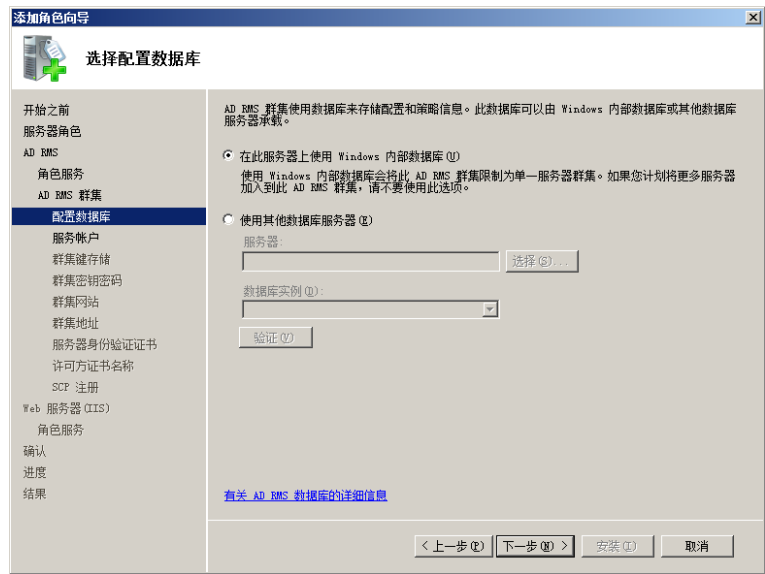


图 17-7 “选择配置数据库”对话框

注意：选择支持 AD RMS 群集的专用数据库时应注意记录其数据库实例，其他 AD RMS 服务器加入群集时也必须指定相同的实例名称。

⑦ 单击“下一步”按钮，显示如图 17-8 所示的“指定服务帐户”对话框。该服务帐户即将来要在 AD RMS 群集中使用的帐户，可使用普通域成员帐户，但必须区别于当前服务器登录的域用户帐户。

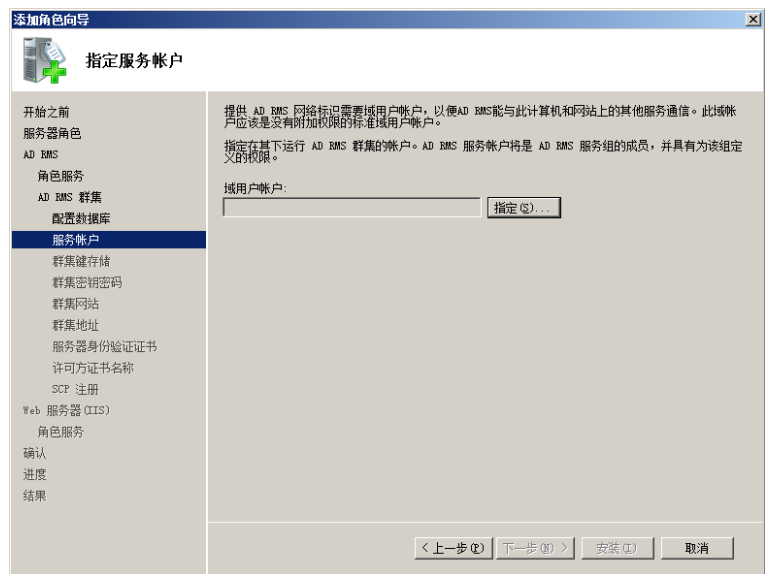


图 17-8 “指定服务帐户”对话框

⑧ 单击“指定”按钮，显示如图 17-9 所示的“Windows 安全”对话框。输入域用户帐户，单击“确定”按钮即可。



图 17-9 “Windows 安全”对话框

⑨ 单击“下一步”按钮，显示如图 17-10 所示的“配置 AD RMS 群集键存储”对话框。系统默认选择“使用 AD RMS 集中管理的密钥存储”单选按钮，即由本地服务器自动生成并存储密钥。这里选择该单选按钮，这个密钥主要用于当前根服务器及将来叶服务器的灾难恢复，必须牢记。选择“使用 CSP 密钥存储”单选按钮，需要由专用加密服务器产生并保管该密钥，比较烦琐，但安全性也相对较高。

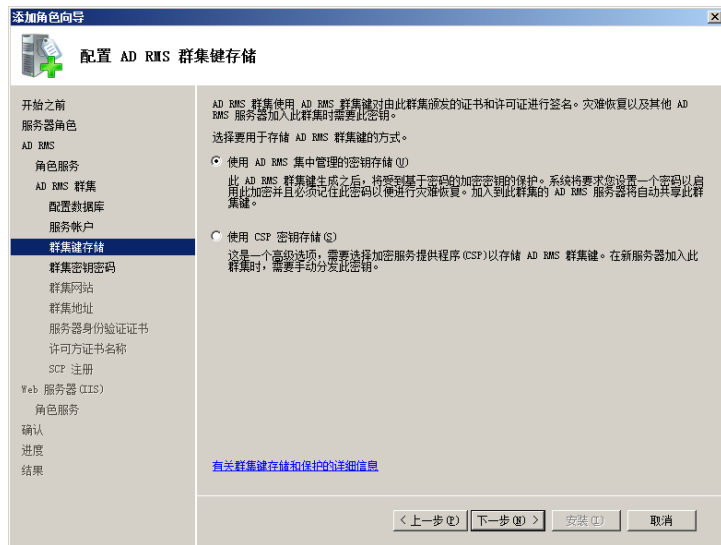


图 17-10 “配置 AD RMS 群集键存储”对话框

⑩ 单击“下一步”按钮，显示如图 17-11 所示的“指定 AD RMS 群集密钥密码”对话框。其他 AD RMS 服务器加入群集时也要使用此密码，必须妥善保存。

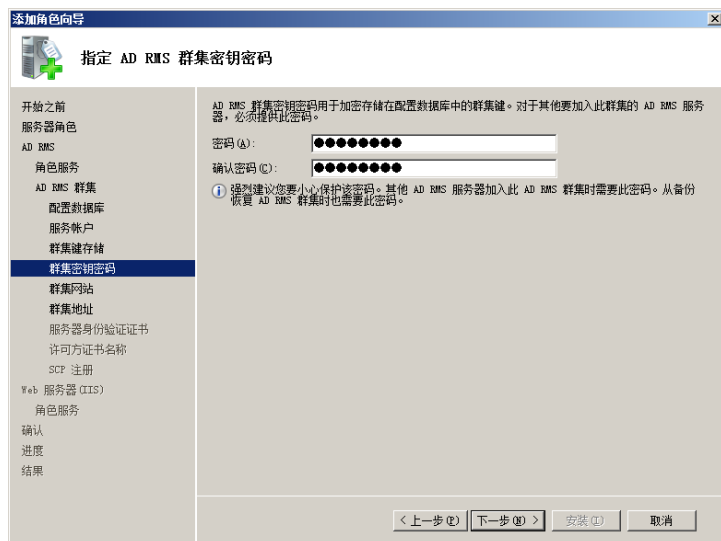


图 17-11 “指定 AD RMS 群集密钥密码”对话框

11 单击“下一步”按钮，显示如图 17-12 所示的“选择 AD RMS 群集网站”对话框。在其中选择管理 AD RMS 群集服务器时使用的站点，准备工作中必须安装 IIS 就是为了在本地创建该站点，保留默认设置即可。

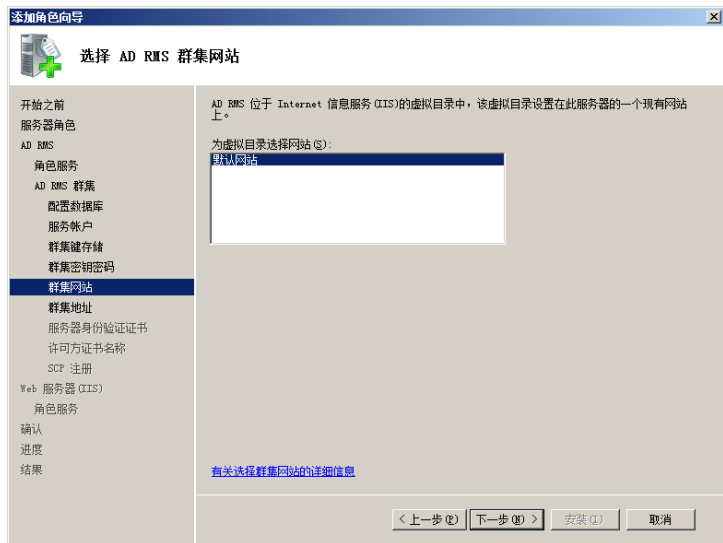


图 17-12 “选择 AD RMS 群集网站”对话框

12 单击“下一步”按钮，显示如图 17-13 所示的“指定群集地址”对话框。群集地址可以使 AD RMS 客户端通过网络与群集通信，选择“使用 SSL 加密的连接”单选按钮。将使用 SSL 加密，客户端只有得到并安装服务器颁发的数字证书后才能建立连接。在“完全限定的域名”文本框中输入要使用的域名，如 https://adrms:443 等。SSL 加密连接使用的默认传输端口是 443，客户端访问时也必须使用完整域名；选择“使用未加密的连接”单选按钮，则使用普通传输方式。输入域名，并单击“验证”按钮。

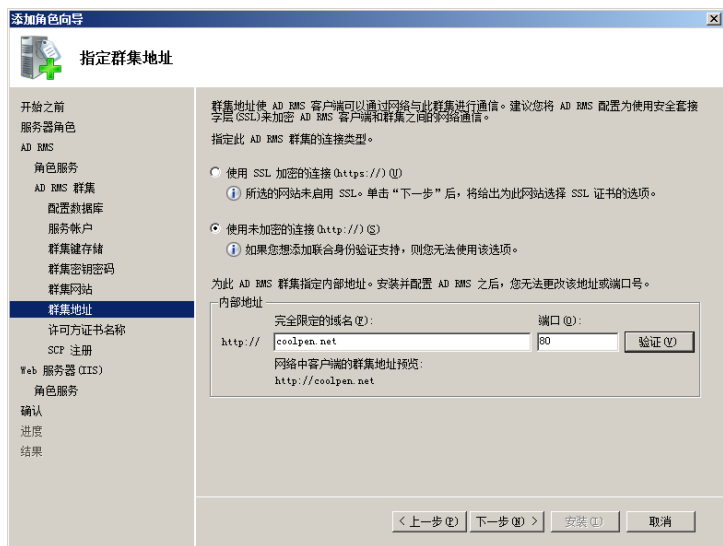


图 17-13 “指定群集地址”对话框

提示

自定义端口也可以提升网络连接的安全性，不过客户端访问时也必须使用相同的端口。

13 单击“验证”按钮，服务器自动验证指定域名和端口的有效性。如果正确，则在“网络中客户端的群集地址预览”下方显示完整域名。

提示 如果选择“使用 SSL 加密的连接”单选按钮，则单击“下一步”按钮会显示如图 17-14 所示的“选择 SSL 加密的服务器身份验证证书”对话框，在其中选择使用某种 SSL 加密方式。

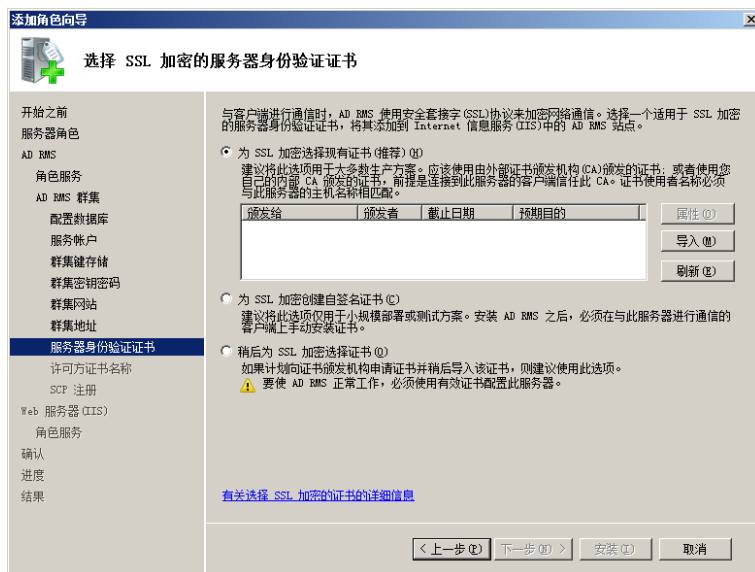


图 17-14 “选择 SSL 加密的服务器身份验证证书”对话框

⑭ 单击“下一步”按钮，显示如图 17-15 所示的“命名服务器许可方证书”对话框。其中显示内容与上述选择的“为 SSL 加密创建自签名证书”单选按钮是对应的，系统默认会以计算机名命名证书，保留默认设置即可。

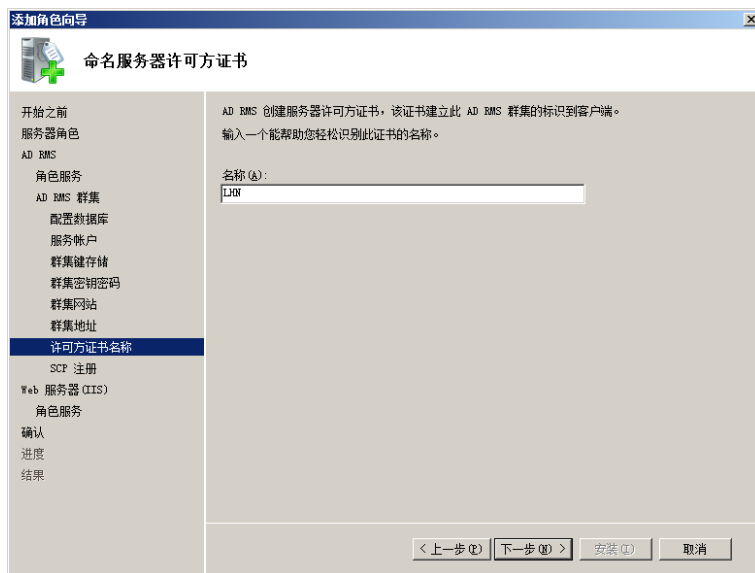


图 17-15 “命名服务器许可方证书”对话框

⑮ 单击“下一步”按钮，显示如图 17-16 所示的“注册 AD RMS 服务连接点”对话框。选择“立即注册 AD RMS 服务连接点”单选按钮，在安装完成后立即开始使用此 AD RMS 群集。

⑯ 单击“下一步”按钮，将显示 IIS 的安装对话框。这里不再赘述。在如图 17-17 所示的“确认安装选择”对话框中显示要安装的组件信息，如果需要修改，单击“上一步”按钮返回。

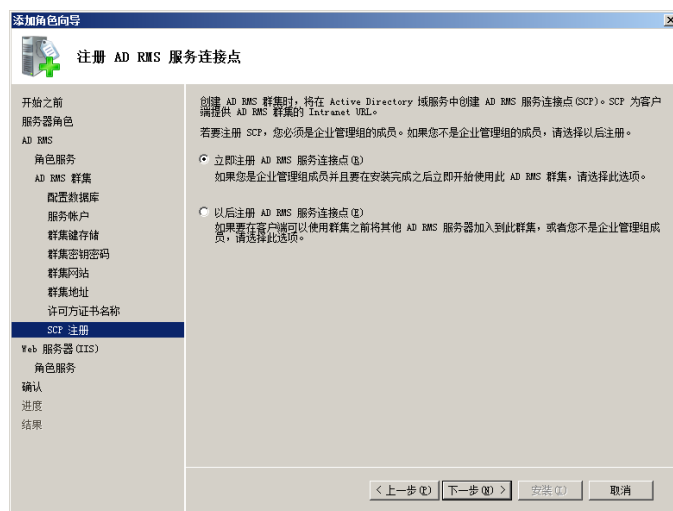


图 17-16 “注册 AD RMS 服务连接点”对话框

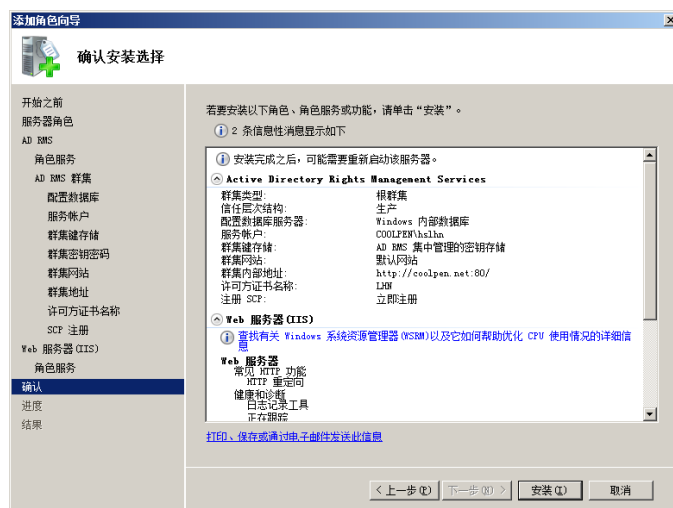


图 17-17 “确认安装选择”对话框

17 单击“安装”按钮开始安装，完成后显示如图 17-18 所示的“安装结果”对话框，提示安装成功。

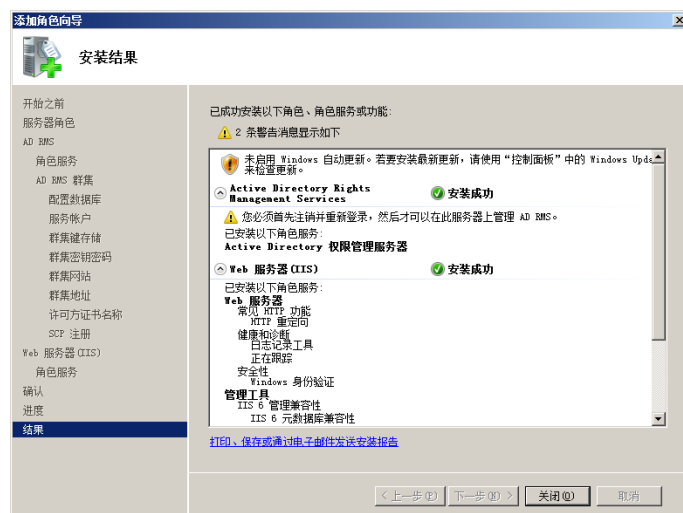


图 17-18 “安装结果”对话框

18 单击“关闭”按钮退出安装向导。然后根据提示注销当前系统并重新登录。

17.2.3 配置 AD RMS 服务器

AD RMS 采用了 MMC 控制台管理的方式，提供文档权限管理服务之前必须经过一些简单配置，如创建信任策略及权限模板等。单击“开始”→“管理工具”→“Active Directory Rights Management Services”选项，启动 AD RMS 控制台，如图 17-19 所示。如果选择 SSL 加密连接方式，则可能会出现“安全警报”提示框，单击“是”按钮跳过即可。

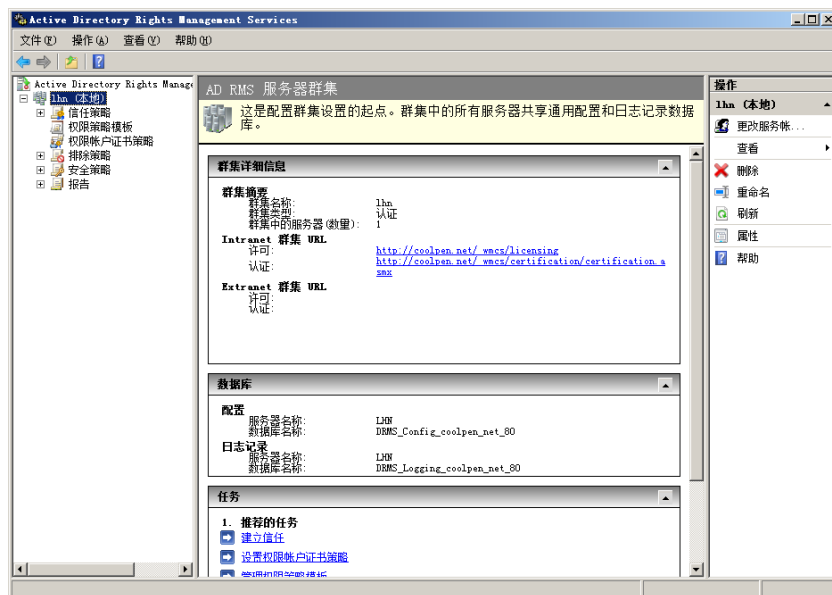


图 17-19 AD RMS 控制台

1. 配置信任策略

信任策略是不同 AD RMS 群集或不同域林中的 AD RMS 服务器之间建立信任关系的唯一标准，主要包括“受信任的用户域”和“受信任的发布域”。

默认情况下，只有受信任的用户域才可以使用当前 AD RMS 服务器提供的权限保护服务，不同 AD RMS 群集或不同林中的 RMS 服务器都是通过彼此的许可证书识别的。用户可以通过将其他 AD RMS 群集中的信任用户域导出，并添加至本地服务器中来实现对其他用户提供权限管理服务。导出的信任用户域文件中会包括原 AD RMS 服务器的许可证信息，因此建立信任关系后来自该域的用户就可以使用当前 AD RMS 服务器提供的使用许可证。

添加受信任的用户域的操作步骤如下。

① 在 AD RMS 控制台窗口中，展开“信任策略”→“受信任的用户域”选项，显示如图 17-20 所示的“受信任的用户域”窗口。在“受信任的用户域信息”列表框中默认显示本地用户域，右击并选择快捷菜单中的“属性”选项即可查看其详细信息。

② 在右窗格的“操作”栏中单击“导入受信任的用户域”超级链接，显示如图 17-21 所示的“导入受信任的用户域”对话框。在“受信任的用户域文件”文本框中输入文件的保存路径，或单击“浏览”按钮选择。在“显示名称”文本框中输入该用户将在列表中显示的名称，用来标识。

③ 单击“完成”按钮，即可完成域的添加，重复操作可添加多个受信任的用户域。

提示 在“受信任的用户域信息”列表框中右击域并选择快捷菜单中的“导出受信任的用户域”选项还可以将其导出，以备本地恢复使用。也可以导入到其他 AD RMS 群集中，用于接受其他 AD RMS 服务器的权限许可证。

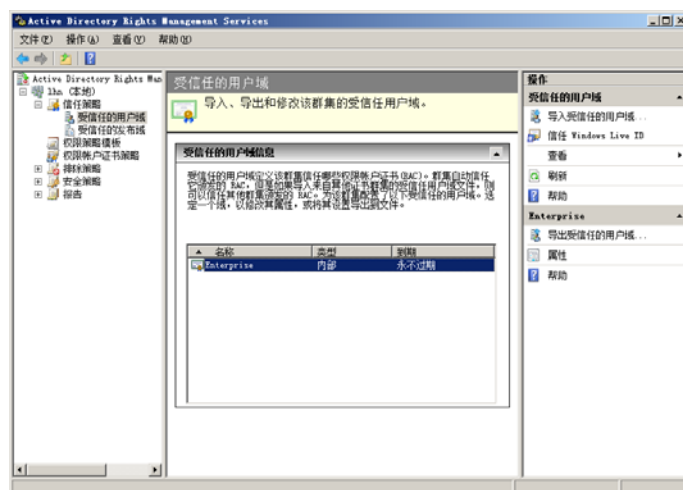


图 17-20 “受信任的用户域”窗口

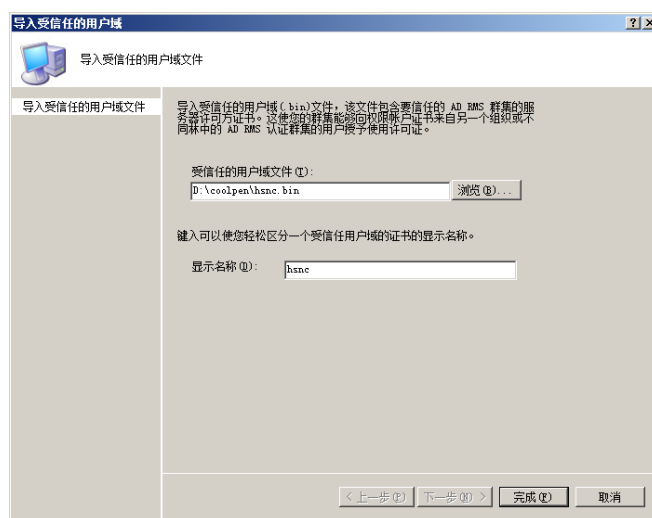


图 17-21 “导入受信任的用户域”对话框

在 AD RMS 控制台窗口中，单击“受信任的发布域”选项，显示如图 17-22 所示的“受信任的发布域信息”窗口。

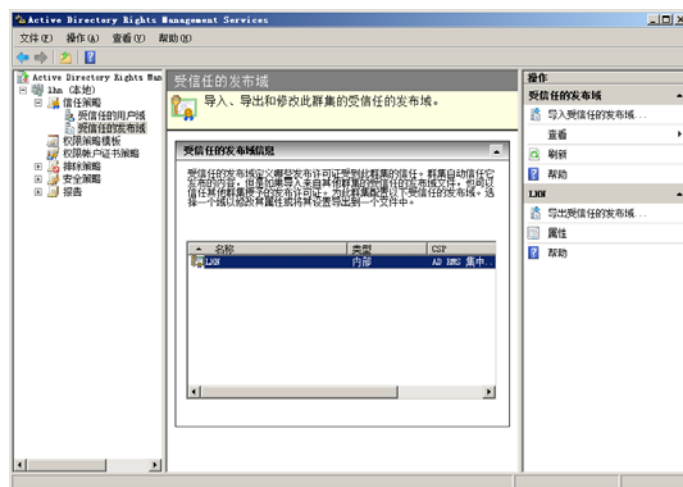


图 17-22 “受信任的发布域信息”窗口

受信任的发布域用于定义那些 AD RMS 群集发布的许可证受到此群集的信任,与受信任的用户域恰恰相反,列表框中默认显示的是本地服务器的记录。受信任的发布域文件的导出和导入与受信任的用户域文件类似,不同的是发布域文件的类型为.XML,其中包括将要信任的 AD RMS 服务器许可方证书、群集密钥和模板等信息。另外,发布域文件本身是受密码保护的,导入时必须输入原 AD RMS 服务器上使用的存储密码。

2. 配置权限策略模板

发布机密程度不同的文档到客户端后设置的权限也有所不同,此时需要为该文档应用不同级别权限的策略模板。权限策略模板是为定义用户的权限策略用的,系统管理员可以通过定制一些现成的策略模板让企业用户直接调用。

创建权限策略模板的操作步骤如下。

① 在 AD RMS 控制台中单击“权限策略模板”选项,显示如图 17-23 所示的“分布式权限策略模板”窗口。

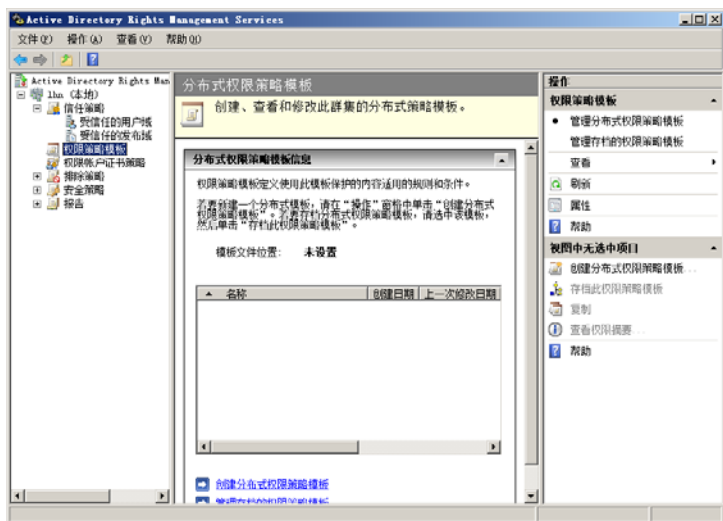


图 17-23 “分布式权限策略模板”窗口

② 单击“操作”栏中的“创建分布式权限策略模板”超级链接,启动创建向导,显示如图 17-24 所示的“添加模板标识信息”对话框。

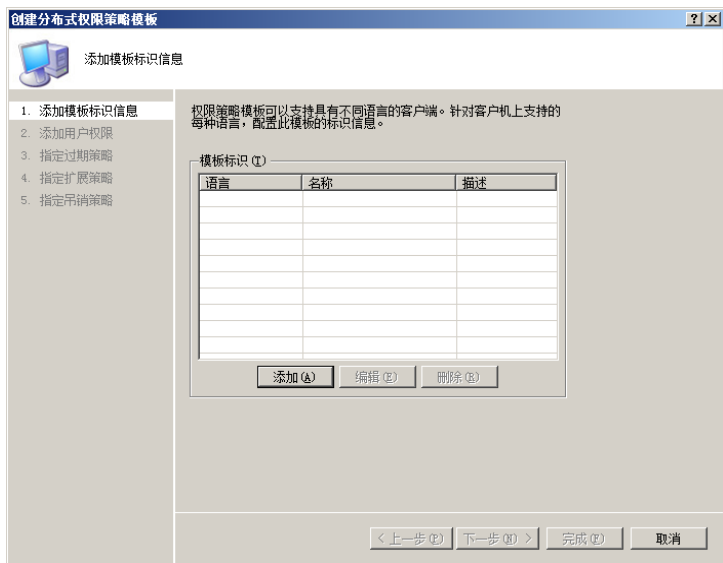


图 17-24 “添加模板标识信息”对话框

③ 单击“添加”按钮，显示如图 17-25 所示的“添加新的模板标识信息”对话框。在“名称”文本框中输入新建模板的名称，在“描述”文本框中输入相关描述信息。单击“添加”按钮，将其添加至“模板标识”列表框中。

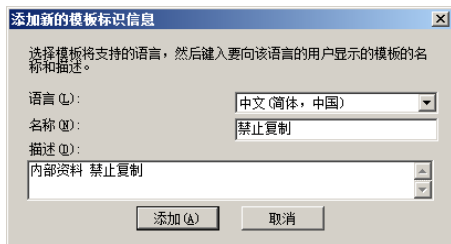


图 17-25 “添加新的模板标识信息”对话框



提示

“语言”下拉列表框是专为使用不同语言的客户端设置的，如果客户端只支持英文显示，则可以在“添加模板标识信息”对话框中再次单击“添加”按钮，并选择“英文”语言即可。需要注意的是，要想使选择的语言生效，必须首先在服务器上安装该语言。

④ 单击“下一步”按钮，显示如图 17-26 所示的“添加用户权限”对话框。默认情况下“用户和权限”列表框为空，即只“授予所有者不会过期的完全控制权限”，其他用户账户没有任何权限。

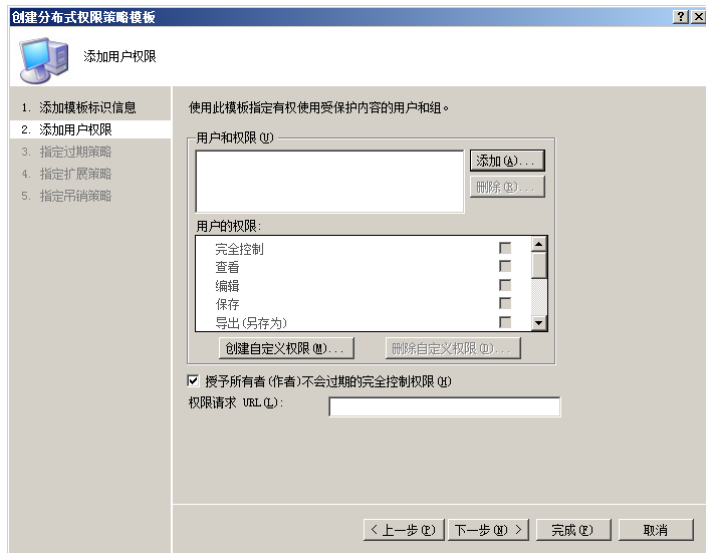


图 17-26 “添加用户权限”对话框

⑤ 单击“添加”按钮，显示如图 17-27 所示的“添加用户或组”对话框。选择“用户或组的电子邮件地址”单选按钮，即可在下面的文本框中输入用户的电子邮件地址。也可以单击“浏览”按钮，打开“选择用户或组”对话框，直接从当前域控制器中查找添加。如果选择“任何人”单选按钮，则对当前域中的所有用户账户有效。

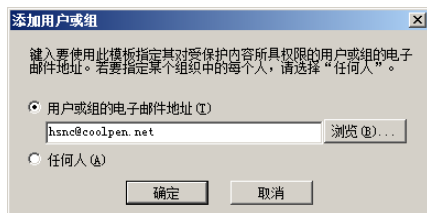


图 17-27 “添加用户或组”对话框

注意：

如果要添加用户，应事先在域控制器上打开用户属性对话框，为用户添加电子邮件地址，如图 17-28 所示。



同样，如果要添加用户组，也要打开用户组属性添加电子邮件地址，如图 17-29 所示。

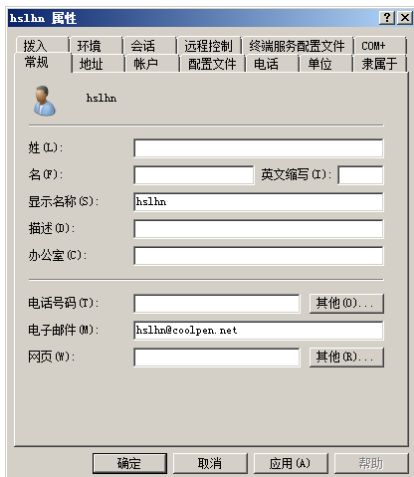


图 17-28 添加用户电子邮件地址

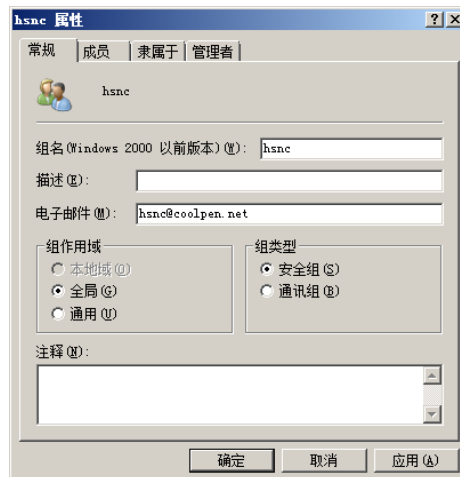


图 17-29 添加用户组电子邮件地址

⑥ 单击“确定”按钮，将所选用户添加至列表框中，如图 17-30 所示。重复操作，可添加多个用户或组的电子邮件地址。然后在“用户和权限”列表中选择赋予用户的权限，例如要求做到“禁止复制”，则只选择“查看权限”复选框即可。



图 17-30 添加用户

“权限请求 URL”是当模板赋予用户的权限无法完成相应工作或在模板权限规定的时间和日期内没有完成工作时，用户可以通过此 URL 继续向管理员发出权限请求，以再次获得权限或附加权限。

注意：

权限列表中给出的所有权限都是允许的，即只要选择某个选项，则表示要赋予用户具有相应的权限。



⑦ 单击“下一步”按钮，显示如图 17-31 所示的“指定过期策略”对话框。在“内容有效期限”选项区域中可以定义当前模板中的权限信息何时过期或有效期限等，默认为“永不过期”。内容过期后，如果仍需要使用该策略信息，则必须重新发布一次。



图 17-31 “指定过期策略”对话框

⑧ 单击“下一步”按钮，显示如图 17-32 所示的“指定扩展策略”对话框。



图 17-32 “指定扩展策略”对话框

在其中设置如下选项。

使用户能够使用浏览器加载项查看受保护的内容：选择该复选框对于没有安装 Office 的客户端是非常实用的，只需安装相关插件即可在浏览器中查看受 RMS 保护的 Office 文档，建议选择该复选框。

每次使用内容时需要更新使用许可证（禁用客户端缓存）：选择该复选框虽然可以使被保护文档更安全，但客户端每次使用时就会非常烦琐。

如果您要为信用 AD RMS 的应用程序指定其他信息，则可以在此处以名称-值对的形式指定：选中该复选框，可在下面的列表框中添加特定应用程序需要的名称和权限值，普通用户无须设置。

⑨ 单击“下一步”按钮，显示如图 17-33 所示的“指定吊销策略”对话框。吊销是 AD RMS 的

一项重要功能，实施之前必须手动创建一个吊销列表。并为每个吊销列表生成一个公钥/私钥对，然后使用私钥签署吊销列表。另外，还必须为吊销列表指定一个用户可以访问的 URL 地址或 UNC 路径。通常情况下，不需要 AD RMS 服务器吊销，即不选择该复选框。

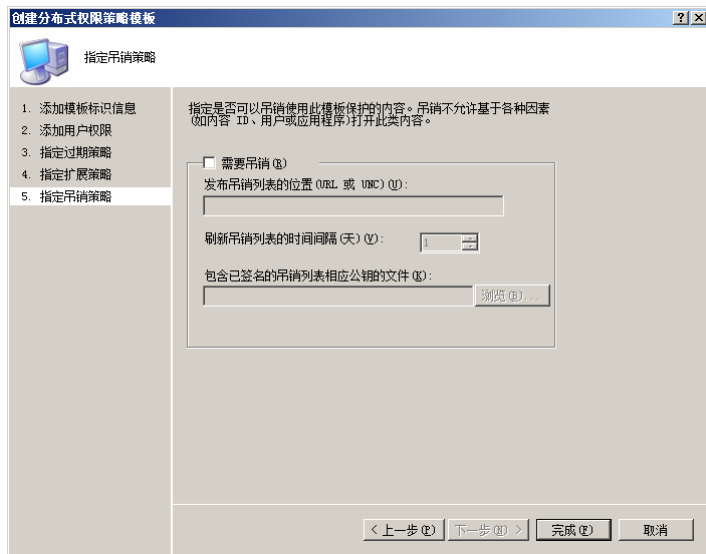


图 17-33 “指定吊销策略”对话框

⑩ 单击“完成”按钮，退出创建向导。返回“公布式权限策略模板”窗口，如图 17-34 所示。新创建的模板已经出现在列表中，此时虽然已经创建成功，但并不能立即应用。

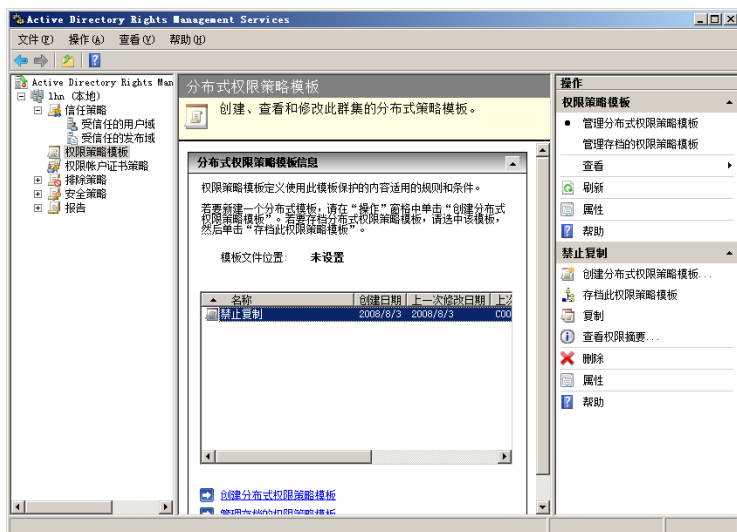


图 17-34 “公布式权限策略模板”窗口

⑪ 选择新创建的策略模板，右击并选择快捷菜单中的“存档此分布式权限策略模板”选项将其本地存档，显示如图 17-35 所示的“存档权限策略模板”对话框。提示一旦保存，将不能再分发或导出该模板。单击“是”按钮保存设置。至此，新创建的权限策略模板才可以保存到本地模板库中备用。

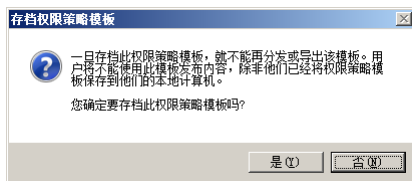


图 17-35 “存档权限策略模板”对话框

⑫ 返回“分布式权限策略模板”窗口，单击“管理存档的权限策略模板”链接，所有已存档的策略模板即可显示在“公布式权限策略模板”列表框中。系统管理员可以继续修改和查看其各项属性信息，如图 17-36 所示为新建策略模板的权限摘要。



图 17-36 新建策略模板的权限摘要

客户端必须将服务器中创建的权限策略模板保存到本地计算机才可以使用，可以通过文件共享、网络传输及移动存储介质等方式获得。默认情况下，权限策略模板的保存位置为“未设置”。为了便于保存和用户使用，应在群集中指定一个公共文件夹，用于保存所有的策略模板。

分发权限策略模板的操作步骤如下。

① 在“公布式权限策略模板”窗口中，单击“操作”栏中的“管理分布式策略模板”超级链接。在“分布式权限策略模板”窗口下方单击“更改分布式权限策略模板文件位置”超级链接，打开如图 17-37 所示的“权限策略模板”对话框。

② 选择“启用导出”复选框，在“指定模板文件位置”文本框中输入已经设置的共享文件夹路径，如图 17-38 所示。注意，这里必须使用 UNC 格式，并且确定已经为指定用户账户赋予了写入权限。

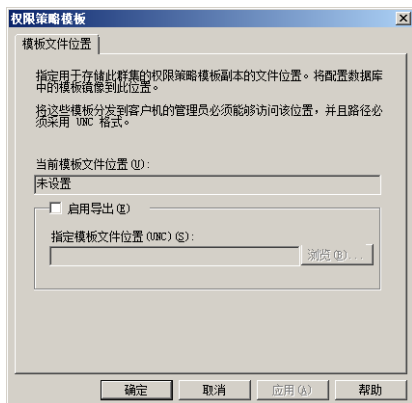


图 17-37 “权限策略模板”对话框

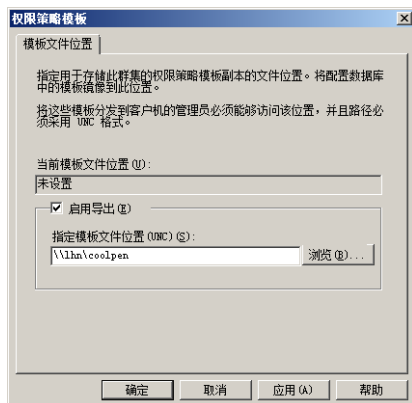


图 17-38 已经设置的共享文件夹路径

③ 单击“确定”按钮，然后单击“管理存档的权限策略模板”超级链接。选择想要分发的模板，右击并选择快捷菜单中的“分发此权限策略模板”选项，显示如图 17-40 所示的“分发权限策略模板”对话框。提示分发之后，用户即可使用此模板发布新内容。

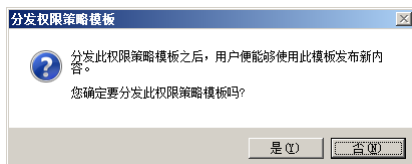


图 17-39 分发权限策略模板

④ 单击“是”按钮确认即可。



提示

如果模板是从另一台 RMS 服务器迁移到此 RMS 服务器的，在使用之前必须由此服务器签署，然后重新分发到客户端。

当某个权限策略模板不再适用时可以将其删除，删除的同时应删除用户计算机中的该模板，以便用户试图使用由已撤销的权限策略模板发布内容时不会出现问题。当作者使用权限策略模板发布内容时，该发布请求将被发送到 RMS 服务器。RMS 将使用数据库中存储的该权限策略模板的副本来响应该请求，如果数据库中不存在该权限策略模板，请求将失败。

要保护重要的权限策略模板，可以将配置数据库中的模板数据定期备份到存储介质中，并存放到安全的地方。这样当系统发生故障时，系统管理员就可以使用备份的副本来恢复权限策略模板。

3. 配置权限账户证书策略

权限账户证书（RAC）是 AD RMS 服务器颁发给每个客户的认证凭证，该证书将用户账户与一个受保护的密钥对关联，而密钥对则专用于用户的计算机。用户可以通过这些证书来发布和使用受 AD RMS 保护的内容，每个证书都包含一个公钥，以向用户授予使用相关信息的权限。

在“AD RMS 控制台”窗口中的左窗格中单击“权限账户证书策略”选项，显示如图 17-40 所示的“权限账户证书策略”窗口。权限账户证书根据有效期的长短和应用环境的不同，可分为标准 RAC 和临时 RAC。标准 RAC 的默认有效期限是 365 天，通常应用于固定用户的计算机上；临时 RAC 的默认有效期限为 15 分钟，主要是为了方便用户在不同位置都可以使用受 AD RMS 保护的文档。

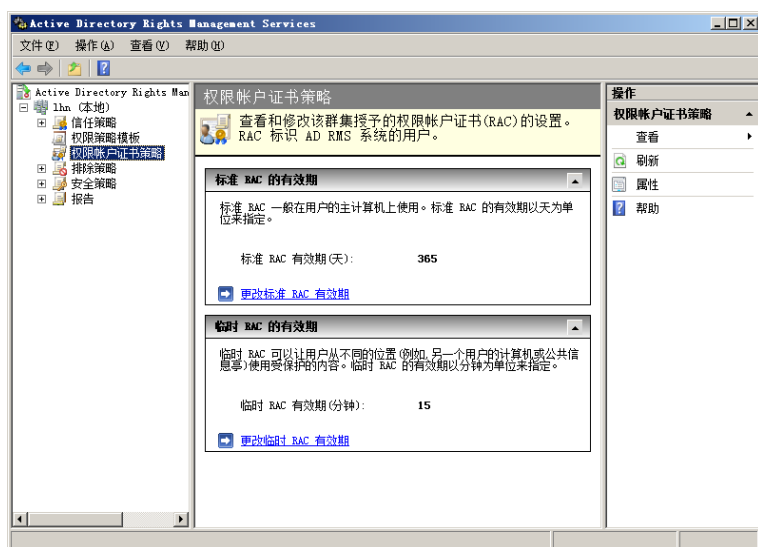


图 17-40 “权限账户证书策略”窗口

权限账户证书的有效期限可以根据实际需要更改，单击“更改标准 RAC 有效期限”超级链接，显示如图 17-41 所示的“权限账户证书策略”对话框。在“标准 RAC 的有效期限（天）”文本框中输入合适数值即可，有效期限的范围是 1~9 999 天。

打开如图 17-42 所示的“临时 RAC”选项卡，或者在“权限账户证书策略”窗口中单击“更改临时 RAC 有效期限”超级链接，也可以更改临时 RAC 的有效期限。

4. 配置排除策略

排除策略的功能是防止非授权用户使用 AD RMS 服务，可供用户使用的排除策略包括用户、应用程序、密码箱版本和 Windows 版本。默认情况下这些策略都是不启用的，配置之前应先将其启用。排除策略排除某个实体后，AD RMS 服务器创建的用户许可证将在排除列表中列出该实体。如果一段时间后决定删除某个以前包含在排除策略中的实体，只需在“排除策略”窗口的相应列表框中将其删除即可，任何获取新证书的请求或授权请求都不会将该实体当做已排除实体。



图 17-41 “权限账户证书策略”对话框

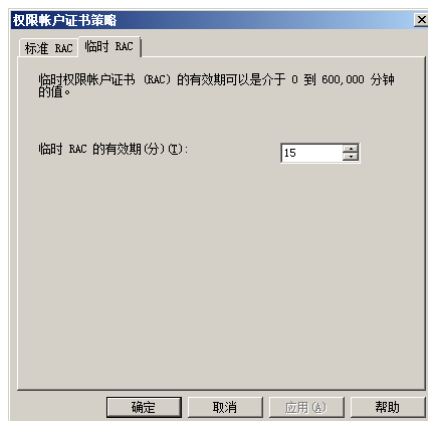


图 17-42 “临时 RAC”选项卡

在 AD RMS 控制台窗口中选择“排除策略”选项，显示如图 17-43 所示的“排除策略”窗口，在其中可以设置用户、应用程序、密码箱及 Windows 版本排除。



图 17-43 “排除策略”窗口



建议不要从排除策略中删除实体，除非可以确定在创建排除策略前颁发的所有证书都已到期；否则新旧证书都将允许对内容解密，留下非常严重的安全隐患。



用户排除可用于排除已经存在安全隐患的信任用户，如某用户账户原本是可信的。但其 AD RMS 凭证不慎泄露，其他非授权用户则可能通过此凭证使用受 RMS 保护的文档，此时就可以通过排除该用户的权限账户证书的公钥来排除该证书。排除权限账户证书后，下次该用户试图获得新内容的用户许可证时，其请求将被拒绝。要获得用户许可证，该用户必须使用新的密钥对来检索新的权限账户证书。

要排除根认证服务器或群集上的权限账户证书，可以在根认证服务器的“排除策略”中指定用户的域账户，并且应当在通过注册子过程注册的所有服务器上同时排除其权限账户证书。

(1) 在 AD RMS 的左窗格中展开“排除策略”选项，选择“用户”选项，显示如图 17-44 所示的“用户排除信息”窗口。默认状态下，用户排除为禁用状态。

(2) 在右窗格的“操作”栏中单击“启用用户排除”超级链接，即可启用用户排除策略，如图 17-45 所示。

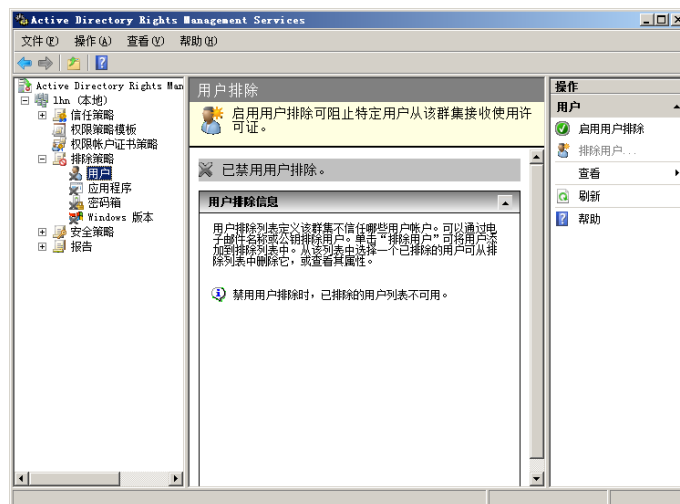


图 17-44 “用户排除信息”窗口

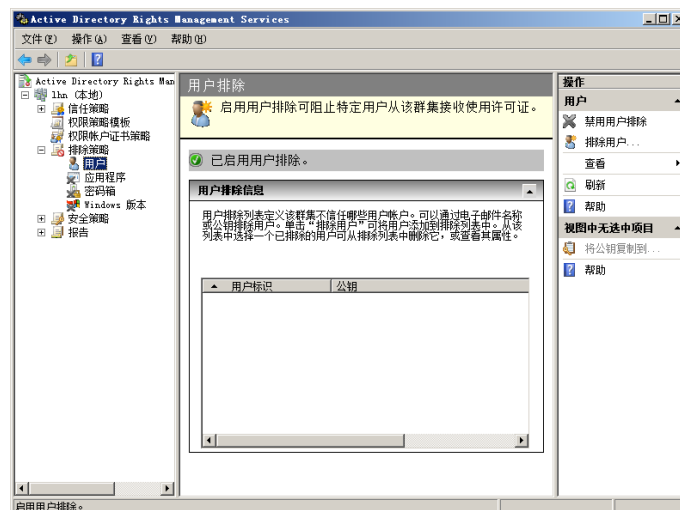


图 17-45 启用用户排除策略

(3) 单击“操作”栏中的“排除用户”超级链接，显示如图 17-46 所示的“添加要排除的用户”对话框，可以通过用户名或者用户账户证书的公钥字符串排除。



图 17-46 “添加要排除的用户”对话框

(4) 单击“完成”按钮，用户排除成功。

排除应用程序的主要依据是应用程序的类型及版本号范围，一旦配置应用程序排除策略，则将在每个用户许可证中添加一个条件限制。即如果请求该许可证的应用程序不在已排除列表中，那么该许可证只能绑定到它所针对的受 AD RMS 保护的内容。应用程序排除在很多情况下都是非常实用的，通常情况下应用程序版本越低，其安全性也越差。通过应用程序排除，就可以限制 AD RMS 服务器为运行较低版本应用程序的客户端提供许可证，以保证文档内容的安全。

(1) 在“排除策略”窗口中选择“应用程序”选项，显示如图 17-47 所示的“应用程序排除”窗口。单击“已启用应用程序排除”超级链接，即可启用应用程序排除。

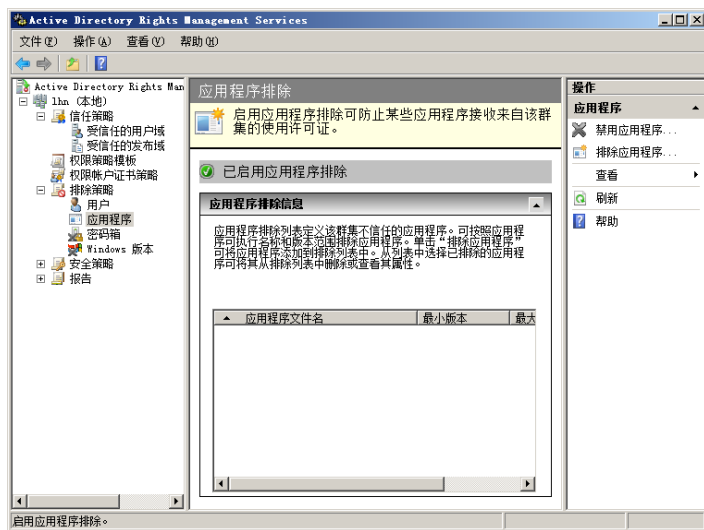


图 17-47 “应用程序排除”窗口

(2) 在“操作”栏中单击“排除应用程序”超级链接，显示如图 17-48 所示的“添加要排除的应用程序”对话框。在“应用程序文件名”文本框中输入应用程序的名称，例如 Office Word 2003。利用“最小版本”和“最大版本”来限定版本范围，必须采用 4 位数字的句点分隔格式，不足 4 位则用零补齐。例如，1.2.3.0。本例中最小 11.5604.5606.0 是未安装 SP2 和 SP3 的 Office，而 11.8169.8172.0 则是 Office 的最新版本。



图 17-48 “添加要排除的应用程序”对话框

(3) 单击“完成”按钮，应用程序排除完成。

密码箱的功能是为客户端提供加密和解密，以保证私钥的安全。密码箱版本小于 AD RMS 指定版本的客户端，将无法从该群集获得权限账户证书或使用许可证。当启用根据密码箱版本排除的功能以后，使用早于指定版本的密码箱软件的客户端将无法获得权限账户证书或用户许可证，原因是其请求将被拒绝。这些客户端必须安装新版本的 AD RMS 客户端软件，以获得使用当前版本软件的新密码箱。

(1) 在“排除策略”窗口中选择“密码箱”选项，单击“操作”栏中的“启用密码箱排除”超级链接即可启用该排除策略，如图 17-49 所示。默认情况下，最小密码箱版本为“未设置”。

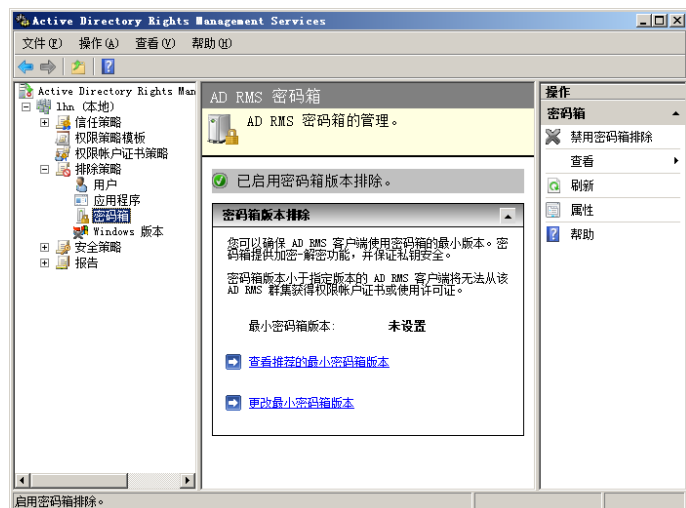


图 17-49 启用密码箱版本排除策略



提示

单击“查看推荐的最小密码箱版本”超级链接，将自动登录微软网站。其中显示最小密码箱版本信息，如图 17-50 所示。

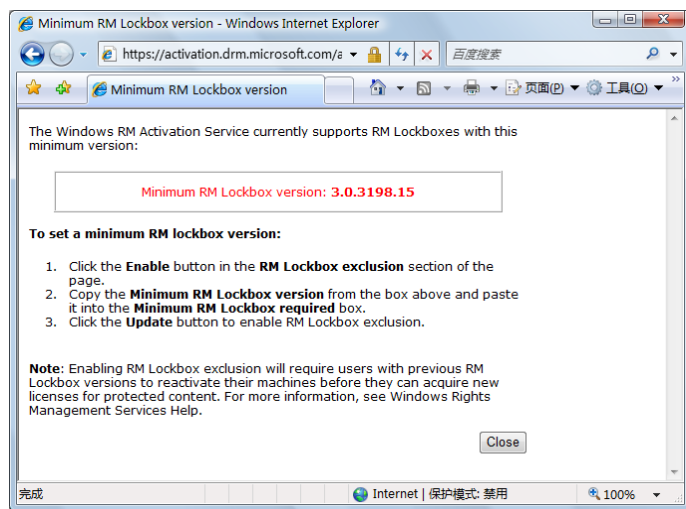


图 17-50 最小密码箱版本信息

(2) 单击“更改最小密码箱版本”超级链接，显示如图 17-51 所示的“密码箱”对话框，在“最小密码箱版本”文本框中输入微软网站反馈的版本信息即可。为了确保服务器的安全，建议不要直接登录网站，可在普通客户端登录该站点并将反馈信息输入服务器即可。

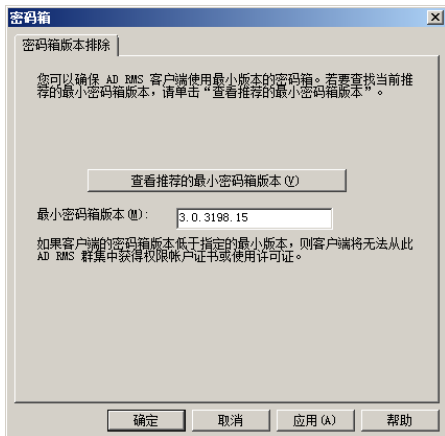


图 17-51 “密码箱”对话框

(3) 单击“确定”按钮，密码箱版本排除成功。

Windows 98 第 2 版或 Windows Me 操作系统支持早期 RMS 1.0 客户端，但是不支持 NTLM 身份验证。因此为了防止用户在运行上述操作系统的计算机上使用受 AD RMS 保护的文档，可以启用 Windows 版本排除策略。使用户只能使用高于 Windows Me 的 Windows 版本，以提高内容的安全性。

在“排除策略”窗口中单击“Windows 版本”选项，显示如图 17-52 所示的“Windows 版本”窗口。单击“操作”栏中的“启用 Windows 版本排除”超级链接，即可启用 Windows 版本排除。

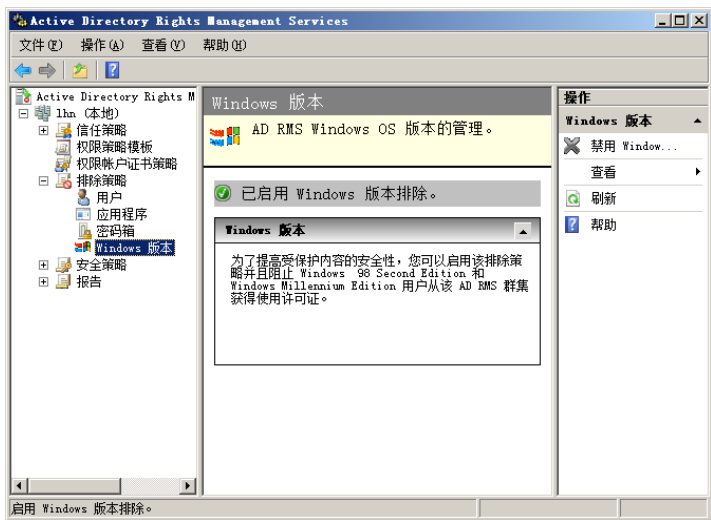


图 17-52 “Windows 版本”窗口

当设置基于 Windows 版本来排除用户的排除策略以后，所有用户许可证中都将包含有相应条件，这些条件可防止运行 Windows 98 第 2 版和 Windows Me 的客户端使用这些许可证。

5. 配置安全策略

在“AD RMS 控制台”窗口的左窗格中选择“安全策略”选项，显示如图 17-53 所示的“安全策略”窗口，其中包括超级用户、群集密钥密码和解除授权。默认状态下，所有策略都是禁用的，配置之前必须将其启用。

超级用户组的成员在从 AD RMS 请求用户许可证时被授予了所有者用户许可证，允许使用该服务器的所有受 RMS 保护的内容。



图 17-53 “安全策略”窗口

(1) 选择“超级用户”选项，在“操作”栏中单击“启用超级用户”超级链接，如图 17-54 所示的“超级用户”窗口启用超级用户。默认情况下，超级用户组为“未设置”。



图 17-54 “超级用户”窗口

(2) 单击“更改超级用户组”超级链接，打开如图 17-55 所示的“超级用户”对话框，在“超级用户组”文本框中输入该 Active Directory 林中现有组的完全限定的域名即可。

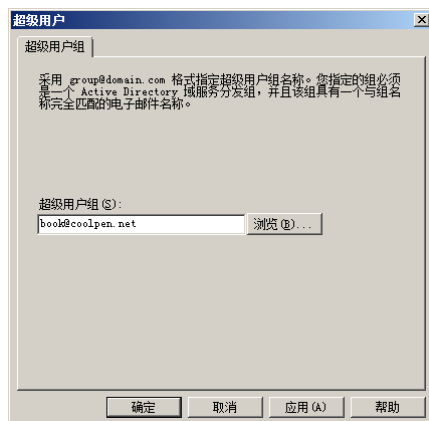


图 17-55 “超级用户”对话框

**注意：**

必须事先在域控制器中，为用户组配置电子邮件名称；否则将无法正常添加。

(3) 单击“确定”按钮，更改超级用户组，如图 17-56 所示。



图 17-56 更改超级用户组

通过设置群集密钥密码，AD RMS 将为服务器创建 AD RMS 私钥。该私钥将被加密并存储在配置数据库中，建议将私钥备份并存储在一个安全的位置。此外，还可考虑使用硬件安全模块来加强 AD RMS 私钥的安全性，因为此密钥将用于受 AD RMS 服务器保护的所有内容的加密模式。如果 AD RMS 私钥由于某种原因被泄露，则需要服务器上取消设置 AD RMS，然后重新设置 AD RMS 以获得新的私钥。

(1) 在“AD RMS 控制台”窗口中选择“群集密钥密码”选项，显示如图 17-57 所示的“群集密钥密码设置”窗口，在其中可以看到密钥保护方法为“AD RMS 集中管理”。

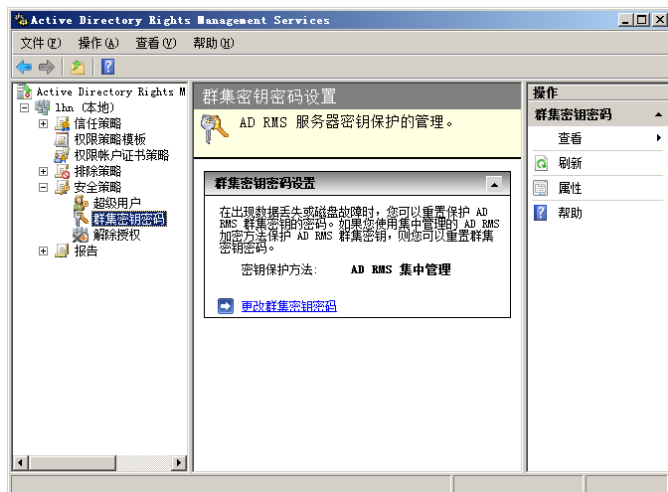


图 17-57 “群集密钥密码设置”窗口

(2) 单击“更改群集密钥密码”超级链接，显示如图 17-58 所示的“群集密钥密码”对话框，分别在“密码”和“确认密码”文本框中输入新的密钥密码。

(3) 单击“确定”按钮，显示如图 17-59 所示的提示框。提示密码已成功重置，单击“确定”按钮即可。



图 17-58 “群集密钥密码”对话框



图 17-59 提示框

注意：

如果该服务器曾用来保护内容，则应通知所有内容所有者使用设置新私钥的 AD RMS 服务器来重新发布内容。使用受已泄露的私钥保护的所有内容副本都应销毁，因为这些内容无法受到足够的保护。



解除授权是指撤销 AD RMS 服务器赋予指定用户对受保护文档的所有权限，即所有用户都具有完全访问的权限。因此通常都是删除 AD RMS 服务器群集时才执行解除授权操作，操作步骤如下。

① 在“安全策略”中选择“解除授权”选项，显示“解除授权”窗口。默认状态下，“解除授权”为禁用状态，并且“解除授权”按钮为灰色不可用状态。单击“操作”栏中的“启用解除授权”超级链接，启用解除授权策略。同时“解除授权”按钮变为可用状态，如图 17-60 所示。



图 17-60 “解除授权”按钮变为可用状态

② 单击“解除授权”按钮，显示如图 17-61 所示的“确认解除授权”对话框。提示如果解除 AD RMS 群集的授权，需要重新安装和配置 AD RMS 群集。

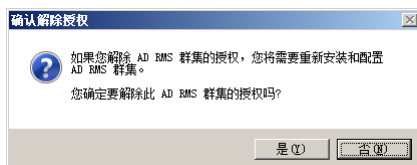


图 17-61 “确认解除授权”对话框

③ 单击“是”按钮即可解除授权，本地 AD RMS 群集的所有配置选项已经被删除，如图 17-62 所示。

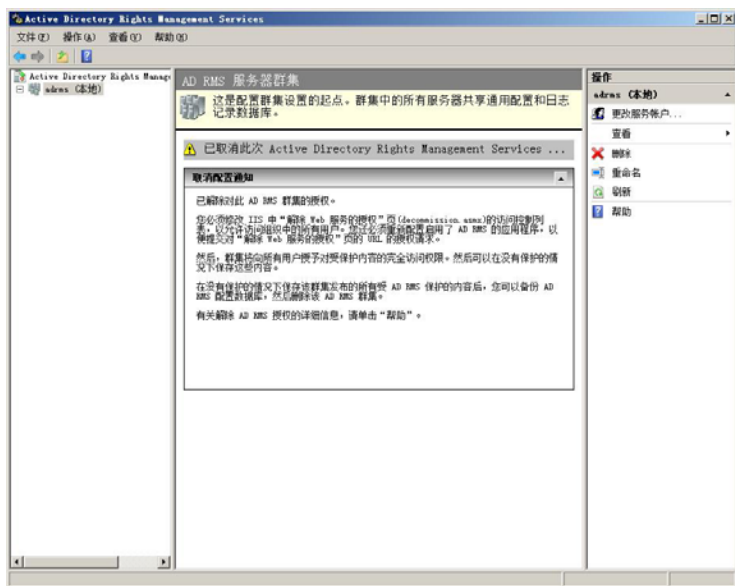


图 17-62 成功解除授权

解除授权后，AD RMS 服务器的操作将会发生改变，它能够提供一个密钥用于解密以前发布的受保护的内容。通过此密钥，可在不使用 AD RMS 保护方法的情况下保存内容。



提示

解除授权之后，还必须修改 IIS 中的“解除 Web 服务的授权”页（decommission.asmx）中的访问控制列表，以允许所有用户访问。在“IIS 管理器”窗口中找到 decommission.asmx 页，并打开如图 17-63 所示的“身份验证”窗口，取消原有的各种身份验证方式，并启用“匿名身份验证”。

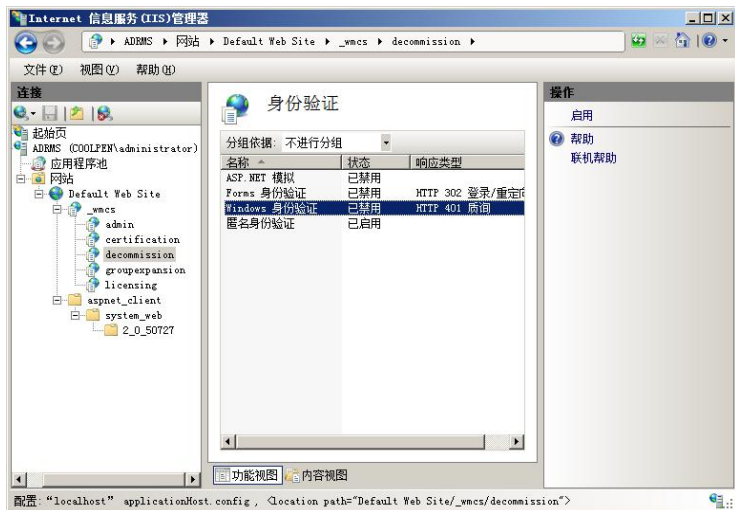


图 17-63 “身份验证”窗口

17.3 安装和配置 AD RMS 客户端

AD RMS 服务安装并配置完成以后，即可将需要接受 AD RMS 管理的客户端加入域并安装和配置 AD RMS 客户端，而后即可利用 RMS 权限来保护 Word 文档。

17.3.1 安装客户端

如果 AD RMS 客户端运行 Windows 2000/XP 系统, 则必须安装客户端程序, 安装完成后无须激活并从服务器下载密码箱。不过该客户端程序并不适用于 Windows Vista 系统, 目前最新版本为 SP2, 简体中文版下载地址为:



图 17-64 安装 RMS 客户端

<http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=02da5107-2919-414b-a5a3-3102c7447838>

下载之后即可安装。另外, 网络管理员还可以通过组策略及 SMS 等方式来向客户端统一分发客户端安装程序。如果客户端数量较少, 则可以通过手动安装的方式实现。

AD RMS 客户端安装过程非常简单, 只需根据向导提示单击“下一步”按钮即可, 如图 17-64 所示, 这里不做详细介绍。需要注意的是, 更换登录的域用户账户后应重新运行客户端安装向导, 并选择“修复带 Service Pack 2 的 Windows Rights Management 客户端”单选按钮。

提示

如果更换了登录的域用户账户, 但仍使用原登录用户的 Office 设置, 则应再次放入 Office 安装光盘。打开“开始”菜单中的“Microsoft Office”程序项, 重新创建当前用户的配置信息; 否则修改客户端注册表时将找不到相关的键值。

安装后需建立客户端到 AD RMS 服务器的连接, 类似于早期版本客户端中的激活。打开或创建一个新的 Office 2003 文档, 单击“文件”→“权限”→“限制权限为”选项。此时客户端自动向 AD RMS 服务器发出申请, 如图 17-65 所示。稍候如果出现“选择用户”对话框, 则表示建立连接成功; 否则表示无法连接到 AD RMS 服务器, 后续的配置也就无从谈起。

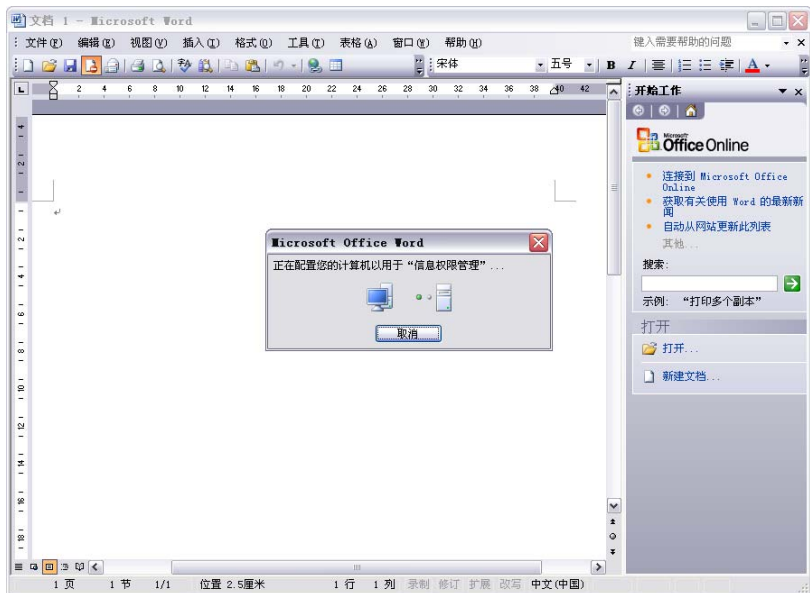


图 17-65 客户端自动向 AD RMS 服务器发出申请

17.3.2 使用 RMS 保护文档

客户端需要将服务器中创建并保存的权限策略模板复制到自己的计算机中才可以使用, 另外还需要在注册表中做相应修改, 操作步骤如下。

① 通过网络共享或移动存储设备，将 AD RMS 服务器上存储的权限策略模板复制到本地计算机上，如图 17-66 所示。

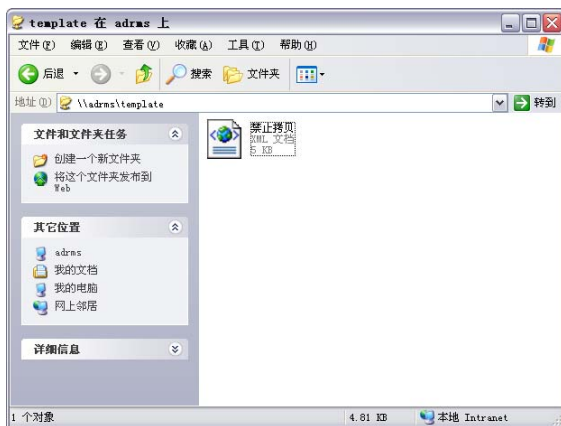


图 17-66 获取权限策略模板

② 打开注册表编辑器，并依次展开如下分支：

HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\DRM

右击右窗格的空白处，选择“新建”→“字符串值”选项。新建一个字符串值对象，如图 17-67 所示。

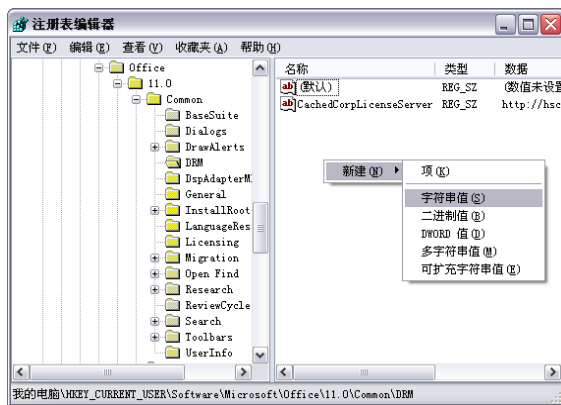


图 17-67 创建字符串值对象

③ 将新创建的字符串值命名为“AdminTemplatePath”，然后双击该对象或右击后选择“修改”选项。打开如图 17-68 所示的“编辑字符串”对话框，指定该对象的数值数据为本地计算机上保存要应用的权限策略模板的路径。这里将要保存在 E 盘根目录下，因此输入“E:\”即可。

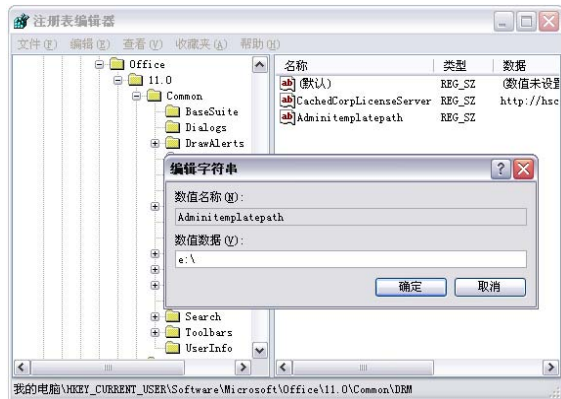


图 17-68 编辑字符串值

④ 单击“确定”按钮保存设置并关闭注册表编辑器窗口，打开要应用此策略模板的受保护文档，打开“文件”菜单中的“权限”选项。此时会发现级联菜单中多出了一个可选项，即“禁止拷贝”，如图 17-69 所示。

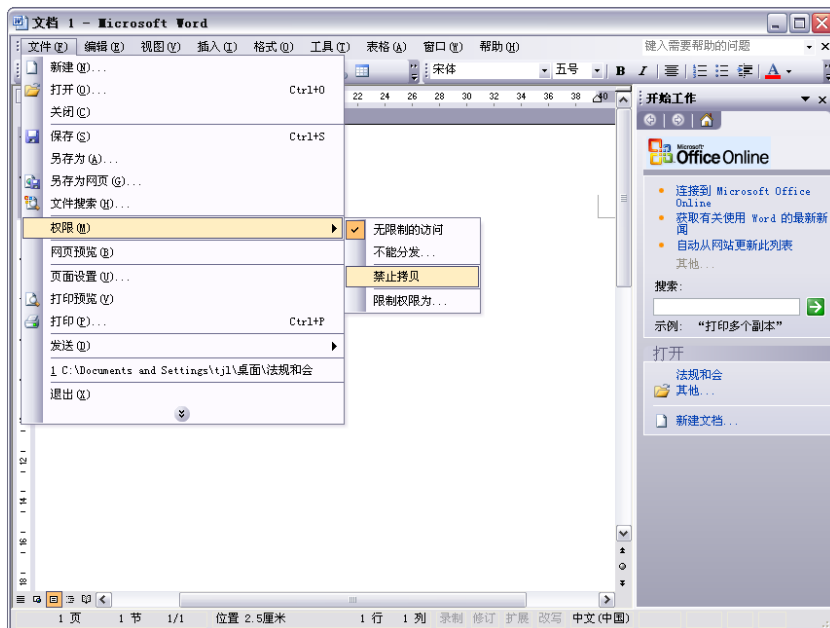


图 17-69 “禁止拷贝”选项

⑤ 选定相应策略模板，共享工作区中会显示如图 17-70 所示的“受限权限”等信息，授权人信息默认是本地登录账户。当然，网络管理员也可以在建立到服务器的连接时指定为其他用户，或单击“更改用户”超级链接随时更改。本例是 lhn@coolpen.net（所用模板针对的用户为 tj1@coolpen.net）。

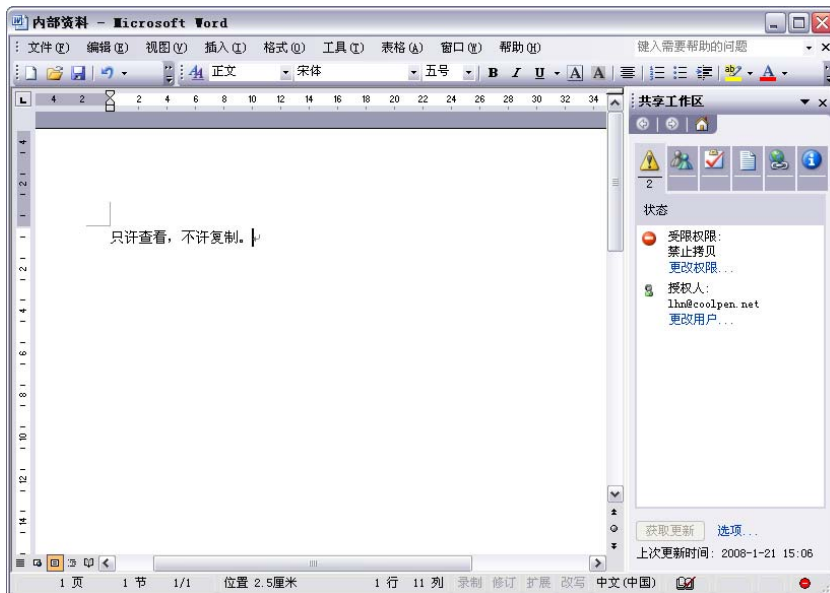


图 17-70 “受限权限”等信息

⑥ 单击共享工作区中的“更改权限”超级链接，可以查看当前用户账户对该文档拥有的控制权限，如图 17-71 所示。由于目前登录用户是该文档的创建者，在 RMS 配置该权限策略模板时为文档作者赋予了完全控制的权限，即所有权限的状态都是“是”。

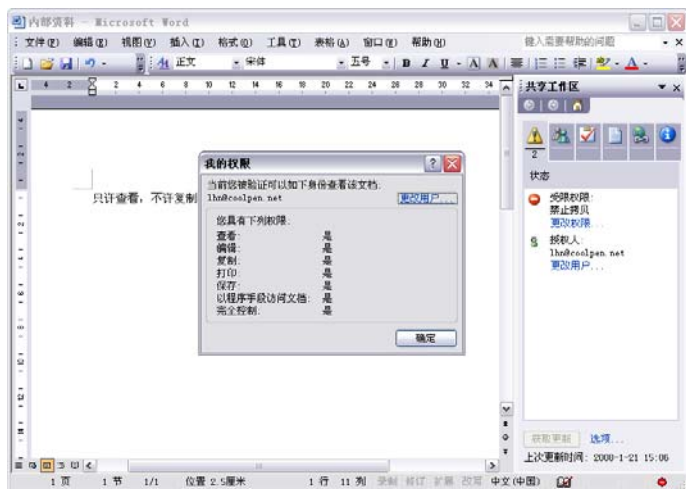


图 17-71 当前用户权限

17.3.3 受限客户端应用被保护文档

AD RMS 策略模板主要是为了限制某些客户端针对文档享有的权限, 因此当这些受限客户端应用被保护文档时, 必须连接到 AD RMS 服务器进行凭据验证并下载相应权限许可证后才可以打开。这里仍以上述应用为例介绍。

(1) 用户 lhn@coolpen.net 创建了文档并应用了限制用户 tj1@coolpen.net 复制和更改的权限, 当用户 tj1@coolpen.net 取得文档并查看时显示如图 17-72 所示的提示框。

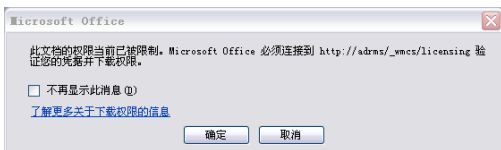


图 17-72 提示框

(2) 单击“确定”按钮, 客户端开始向 AD RMS 服务器提交身份验证并获得相应的权限。最终打开文档, 提示文档是“只读”状态, 并且不允许用户执行“复制”命令, 或按 **PrtSc** 键抓取屏幕, 如图 17-73 所示。这是因为当前被保护文档应用的权限策略模板已经屏蔽了 Windows 的这些功能, 关闭受保护文档则一切恢复正常, 用户使用时应注意。

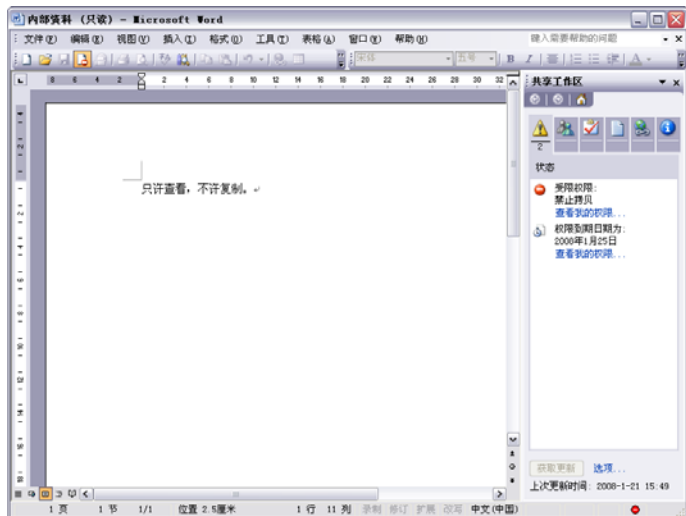


图 17-73 文档为“只读”状态

(3) 单击“查看我的权限”超级链接，打开如图 17-74 所示的“我的权限”对话框。其中只有“查看”一项处于“是”状态，其他均为“否”。

(4) 单击“更改用户”按钮，打开如图 17-75 所示的“选择服务”对话框。如果当前拥有的权限无法正常完成工作，可以选择其中一种方式添加其他有足够权限的用户账户。选择“使用 Microsoft .NET Passport 账户”单选按钮，可以凭借有效的 Microsoft .NET Passport 账户从 Microsoft 获得一个证书实现相应目的，这与 AD RMS 服务器的设置有关。如果添加了 .NET Passport 类型的可信任用户域，则客户端可以使用这种方式；否则无效。选择“使用 Microsoft Windows 账户”单选按钮，即可从当前域中选择其他用户账户来完成相应操作。

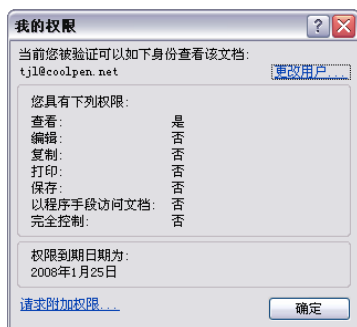


图 17-74 “我的权限”对话框

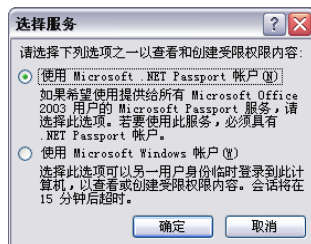


图 17-75 “选择服务”对话框

如果上述方法仍不能获得相应权限，则可以在“我的权限”对话框中单击“请求附加权限”按钮，向 AD RMS 服务器申请相关权限，打开如图 17-76 所示的“申请权限”窗口。“收件人”文本框中为 AD RMS 服务器上设定的接收申请的电子邮件地址，保持默认即可。根据实际需要，说明要请求的权限即可。



图 17-76 “申请权限”窗口



提示

需要应用此功能时，必须首先在网络中配置 Exchange 或其他邮件服务器。虽然在 AD RMS 系统中用到 E-mail 地址的地方非常多，但是多数情况下是作为一种用户标识并非真正地用来传递信息，所以网络中的邮件服务器也就可有可无。如果确实需要传递信息，则必须搭建邮件服务器。

17.3.4 应用 RMS Toolkit

RMS Toolkit 是和 RMS 服务管理程序配套的工具包，主要用于诊断和排除 RMS 应用过程中的各种故障。它只能安装在 RMS 服务器端，但是其中有许多小工具可以在客户端执行并提供较强的诊断

功能。建议完成安装后将 RMS Toolkit 安装目录共享，以备客户端下载。RMS Toolkit 的下载地址为：
<http://www.microsoft.com/downloads/details.aspx?FamilyID=bae62cfc-d5a7-46d2-9063-0f6885c26b98&DisplayLang=en>

RMS Toolkit 的安装非常简单，安装完成打开 RMS Toolkit 安装目录。其中该工具包中提供的命令行工具，如图 17-77 所示，应用较多的是 GetRMScp。

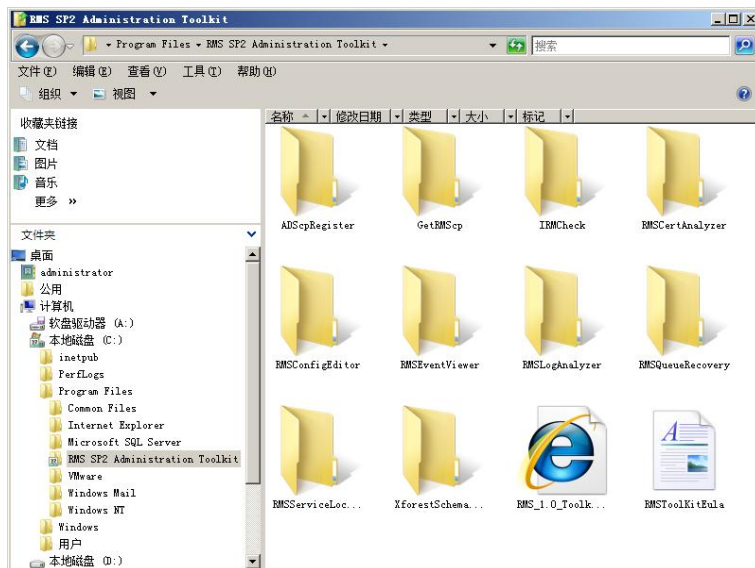


图 17-77 RMS Toolkit 中包括的工具

RMSCheck 的主要功能是检查 RMS 客户端的配置情况，无须复制到本地计算机，直接运行服务器的共享文件即可。

运行 IRMCheck.exe 后会显示命令执行窗口，并在当前客户端系统中检查针对于 RMS 的配置情况，如图 17-78 所示。检查可能需要较长的时间，用户需要耐心等待。

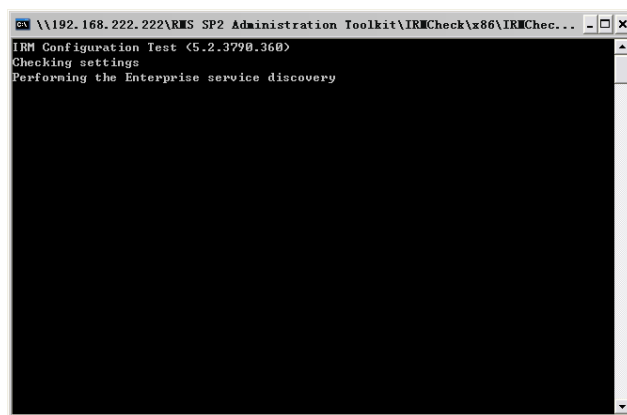


图 17-78 正在检查 RMS 客户端配置

稍等即可返回一个详细的结果报表，如图 17-79 所示，其中包括诊断日期、主机名、当前登录用户账户、操作系统等主机信息，以及 RMS 相关的客户端状态信息。例如，RMS 支持应用程序、客户端版本、客户端激活状态、连接 URL 及证书申请情况等。如果运行正常，则会在“Status”（状态）栏中显示为“SUCCESS”；否则会显示为红色的“ERROR”（错误）。从中可以检查存在问题的环节，从而快速排除故障。

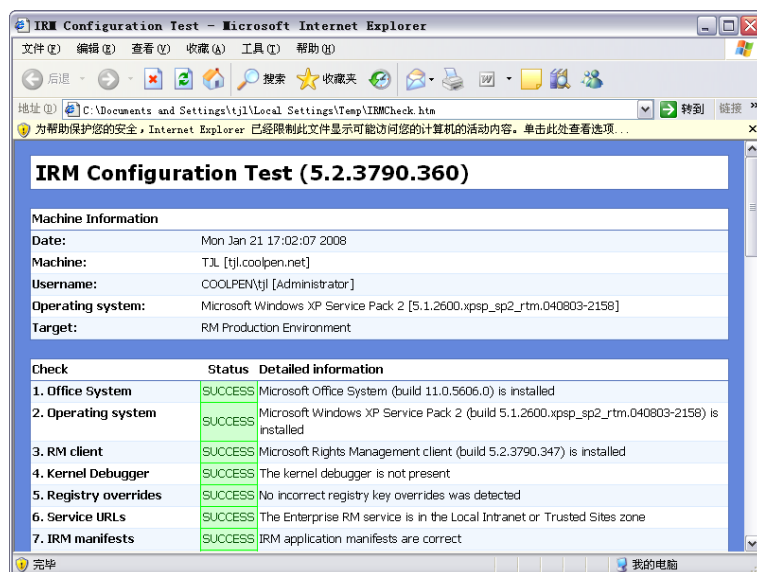


图 17-79 诊断结果报表

17.3.5 应用非常规客户端

所谓非常规客户端主要是指 RMS SP2 客户端安装程序支持的应用程序之外的其他客户端，例如 Office 版本过低或没有安装 Microsoft Office 的用户等。这些用户可以通过安装简单插件即可实现与常规客户端相同的应用，该插件即微软提供的 Add-on。其使用非常简单，这里不再介绍。下载地址如下：

<http://www.microsoft.com/downloads/details.aspx?FamilyId=B48F920B-5AF0-46B4-994F-2F62582CC86F&displaylang=en>



提示

当需要让客户端在 IE 浏览器中查看 Office 文档时，需要在权限策略中指定“使用户能够使用浏览器加载项查看受保护的内容”。

第 18 章 MOM 管理服务器

随着网络的发展，企业涉及的网络业务越来越多，同时也要使用更多的服务器。但是网络管理人员通常不会增多，从而造成管理工作繁重且效率降低。为了解决这种管理困境，微软公司开发了一套企业 IT 数字管理系统——Microsoft Operations Manager 2005。用其可以实现对服务器集中而有效的管理，及时监控服务器，甚至每台服务器的运行状态。为网络管理员提供发生问题的原因及历史记录，并预测即将可能发生的问题。

18.1 MOM 概述

Microsoft Operations Manager 2005（简称“MOM 2005”）是一种管理软件，它通过管理规则及预定义的计算机组按照预定义的事件、警报和性能规则，并提供的脚本完成目标服务器系统的监控，有助于管理基于 Windows 网络 and 应用程序的可用性、安全和性能。

►► 18.1.1 监控模式

MOM 2005 提供了两种监控模式，分别为被动式监控和主动式监控。

（1）被动式监控：MOM 2005 监控企业中所有受管理服务器，当监控到符合系统设置的事件规则及警报规则时，立即响应。即以电子邮件或消息通知等方式通知网络管理员，或者呈现在 MOM 2005 的操作控制台中。

（2）主动式监控：通过定义的 Script 脚本主动检查企业未来环境中的服务器或者代理管理的服务器系统中重要服务的状态，例如 Active Directory 数据库日志是否正常及磁盘空间是否足够使用等。若主动检查出问题，会同被动式监控一样发出警告。

►► 18.1.2 MOM 服务器

管理服务器是 MOM 2005 体系中的服务器端应用程序，包括以下组件。

（1）数据存取服务器组件：作为 MOM 2005 管理服务器与 MOM 2005 数据库间的中介数据存取的 COM+ 组件。

（2）MOM 2005 服务器：MOM 2005 代理程序通过 MOM 2005 服务器组件从 MOM 2005 管理服务器取得当前状态以及规则等相关信息，MOM 2005 代理程序通过 MOM 2005 Server 组件将收集到的数据传送给 MOM 2005 管理服务器，MOM 2005 管理服务器再由 MOM 2005 服务器组件通过数据存取组件存取 MOM 2005 数据库中的数据。

（3）MOM 2005 本地代理组件：执行发现计算机及安装 MOM 2005 远程代理程序并监控无代理程序管理计算机。

►► 18.1.3 MOM 数据库

MOM 2005 使用 SQL Server 作为后台数据库，默认数据库名称为“OnePoint”。在 MOM 2005 数据库中存放以下两种类型的数据。

（1）Configuration Data：静态的设置数据，例如管理包中各个规则的设置和通用设置等。

（2）Operational Data：动态数据，例如，由 MOM 2005 代理程序回传的数据。

18.1.4 报表服务

不同的管理包都会有对应的报表，其中包含系统监控及运行报告、容量规划报告及性能分析报告，以及应用程序相关监控报告等。

在安装 MOM 2005 报表服务组件时，在指定的 SQL Server 实例中建立一个数据库，数据库名称为“SystemCenterReporting”。MOM 2005 报表服务通过 SQL DTS 定时地将数据从 MOM 2005 数据库（OnePoint）转换至 SystemCenterReporting 数据库，同时也在 SQL Reporting Service 平台上建立链接至 SystemCenterReporting 数据库所需的数据。如果在导入管理包向导中选择导入报告，就会在 SQL Reporting Service 平台上建立链接至 SystemCenterReporting 的报表。

使用 SQL Reporting Service 平台的优点是可以使用 Reporting Service 既有的功能，也可以使用 Visual Studio .NET 开发定制化的报表。

18.2 安装 MOM

要正常使用 MOM 2005，必须在服务器和客户端上分别安装服务器端和客户端程序。服务器端必须使用 Windows 2000、Windows Server 2003 或 Windows Server 2008 操作系统，并且已加入到域；而 MOM 客户端则应采用 Windows 2000、Windows XP 或 Windows Vista 操作系统。

18.2.1 安装 MOM 前的准备工作

为了保证 MOM 的顺利安装，在安装 MOM 之前应配置好 MOM 服务器。并安装所需要组件并检查先决条件，以免在安装 MOM 时出现错误。

1. 安装所需组件

在安装 MOM 2005 前应做好如下准备工作。

(1) 将 MOM 服务器加入域。

(2) 安装 IIS 和 ASP.NET 组件。

(3) 安装 SQL Server，必须为 SQL Server 2000 SP3 以上版本。此处使用 SQL Server 2005。安装完成以后，必须将“SQL Server”和“SQL Server Agent”服务的“启动类型”设置为“自动”，并启动这两个服务，如图 18-1 所示。

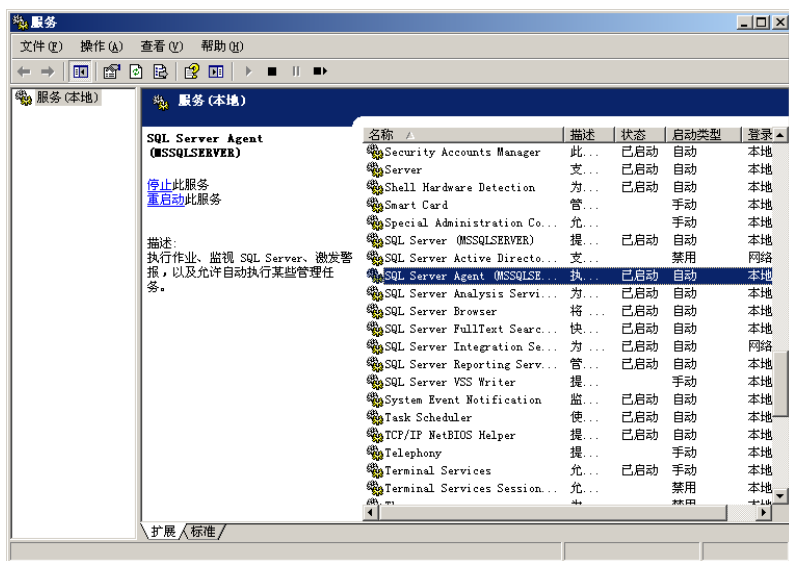


图 18-1 启动 SQL Server 服务

2. 检查先决条件

MOM 2005 自带的“检查先决条件”功能可以检测当前服务器的软件和硬件是否满足 MOM 2005 的需求。如果有的条件不符合，系统管理员需要重新配置服务器，操作步骤如下。

① 将 Microsoft Operations Manager 2005 安装光盘放入光驱，自动启动 MOM 程序，显示如图 18-2 所示的“Microsoft Operations Manager 2005 安装程序资源”对话框。

② 单击“检查先决条件”超级链接，显示如图 18-3 所示的“检查先决条件”对话框。选择“Microsoft Operations Manager 2005 组件”单选按钮，同时选中“MOM 2005 数据库”、“MOM 2005 管理服务器”和“MOM 2005 用户界面”复选框。



图 18-2 “Microsoft Operations Manager 2005 安装程序资源”对话框

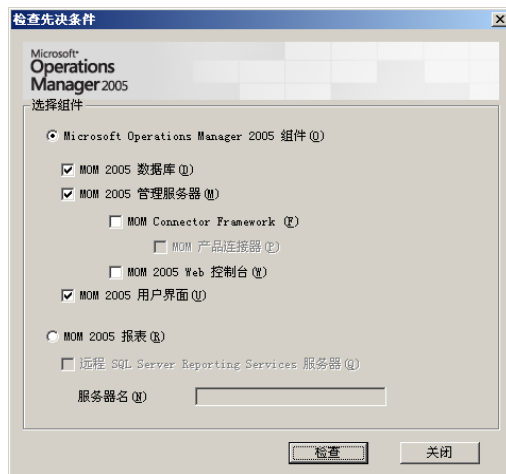


图 18-3 “检查先决条件”对话框

③ 单击“检查”按钮，显示如图 18-4 所示的“Microsoft Operations Manager 2005 组件”窗口，显示检查结果。

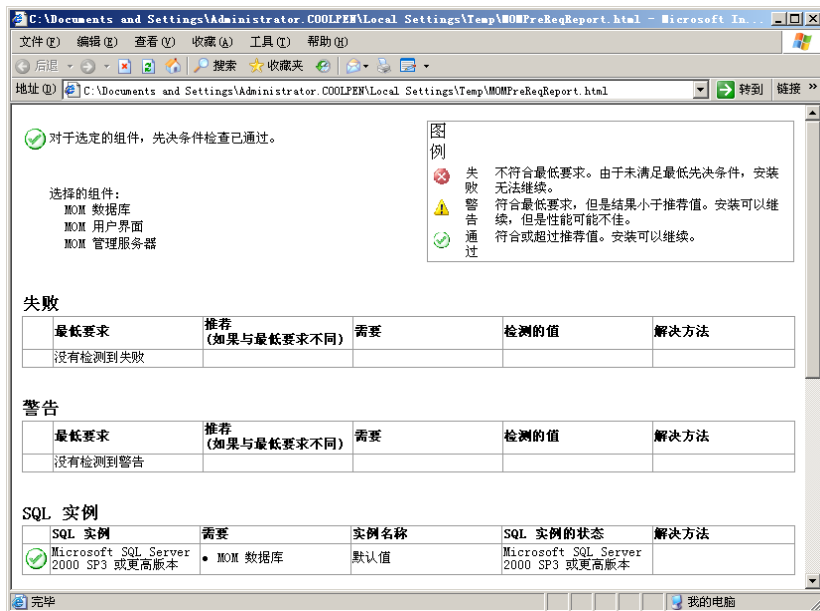


图 18-4 “Microsoft Operations Manager 2005 组件”窗口

- 失败（红色叉号）：不符合最低要求，安装无法继续。
- 警告（黄色感叹号）：符合最低要求，但是结果小于推荐值。
- 通过（绿色对勾）：符合或超过推荐值。

根据检查结果，可以发现当前服务器配置是否符合 MOM 2005 的安装要求。如果符合，可以开始安装；否则应检查服务器软硬件配置，直到符合要求为止。

18.2.2 安装 Microsoft Operations Manager 2005 组件

安装 Microsoft Operations Manager 2005 组件的操作步骤如下。

① 在“Microsoft Operations Manager 2005 安装程序资源”对话框中，单击“安装 Microsoft Operations Manager 2005”超级链接，打开“Microsoft Operations Manager 2005 安装程序”向导，如图 18-5 所示。

② 单击“下一步”按钮，显示如图 18-6 所示的“最终用户许可协议”对话框，选择“我接受许可协议中的条款”单选按钮。



图 18-5 “Microsoft Operations Manager 2005 安装程序”向导



图 18-6 “最终用户许可协议”对话框

③ 单击“下一步”按钮，显示如图 18-7 所示的“产品注册”对话框。在“用户名”和“单位”文本框中键入用户名和用户所在的单位，在“输入 25 位的 CD 序列号”文本框中键入 MOM 2005 的产品序列号。

④ 单击“下一步”按钮，显示如图 18-8 所示的“安装选项”对话框。选择合适的安装类型，一般情况下使用默认值即可。

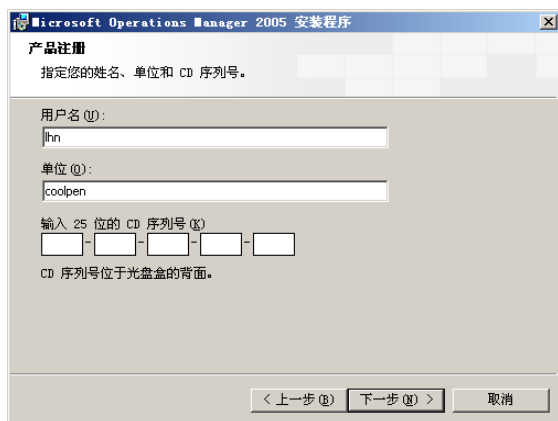


图 18-7 “产品注册”对话框



图 18-8 “安装选项”对话框

⑤ 单击“下一步”按钮，显示如图 18-9 所示的“已通过先决条件检查”对话框。

⑥ 单击“下一步”按钮，显示如图 18-10 所示的“SQL Server 数据库实例”对话框，选择 SQL Server 数据库实例。

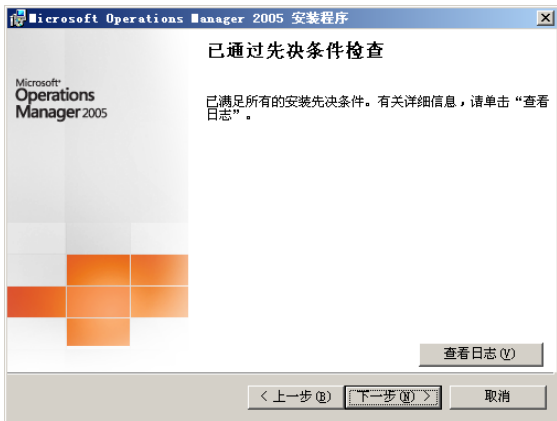


图 18-9 “已通过先决条件检查”对话框

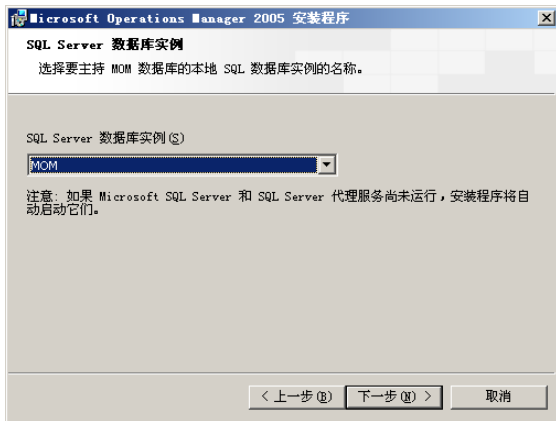


图 18-10 “SQL Server 数据库实例”对话框

⑦ 单击“下一步”按钮，显示如图 18-11 所示的“数据库和日志文件选项”对话框。在“数据库大小”文本框中键入数据库文件的初始大小，默认值为 1000 MB，这里保持默认设置。默认数据库文件和日志文件的安装位置是 Microsoft Sql Server 2000 或者 Microsoft Sql Server 2005 数据库默认安装位置。

⑧ 单击“下一步”按钮，显示如图 18-12 所示的“管理组名称”对话框。在“管理组名称”文本框中键入管理组名称，这里为 Coolpen。



图 18-11 “数据库和日志文件选项”对话框



图 18-12 “管理组名称”对话框

⑨ 单击“下一步”按钮，显示如图 18-13 所示的“管理服务器操作账户”对话框。在“用户账户”和“密码”文本框中键入可以管理 Microsoft Operations Manager 2005 的账户和密码，在“域或本地计算机”下拉列表框中选择域名。

⑩ 单击“下一步”按钮，显示如图 18-14 所示的“数据访问服务器账户”对话框。提议数据访问服务器账户使用专用账户，这里使用域账户 Inn。

⑪ 单击“下一步”按钮，显示如图 18-15 所示的“许可证”对话框，在“MOM 管理许可证数”文本框中键入许可证数量。

⑫ 单击“下一步”按钮，显示如图 18-16 所示的“MOM 错误报告”对话框，保留默认设置即可。

⑬ 单击“下一步”按钮，显示如图 18-17 所示的“Active Directory 配置”窗口。如果所有计算机都处于域，选择“是，所有计算机均位于相互信任的 Active Directory 域。(推荐)”单选按钮。

⑭ 单击“下一步”按钮，显示如图 18-18 所示的“已准备好安装”对话框。

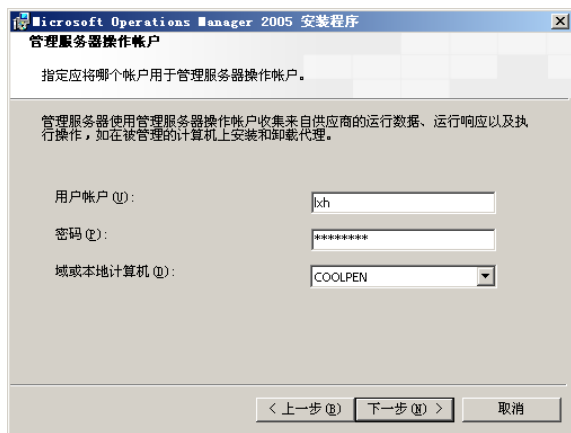


图 18-13 “管理服务器操作账户”对话框

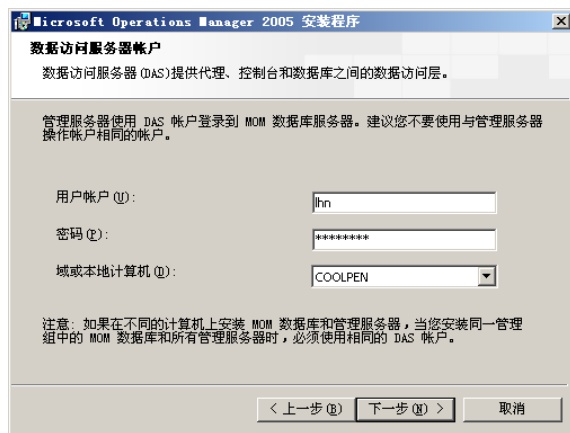


图 18-14 “数据访问服务器账户”对话框



图 18-15 “许可证”对话框

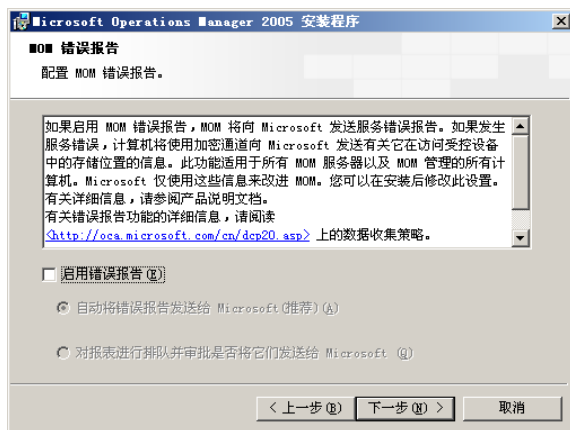


图 18-16 “MOM 错误报告”对话框

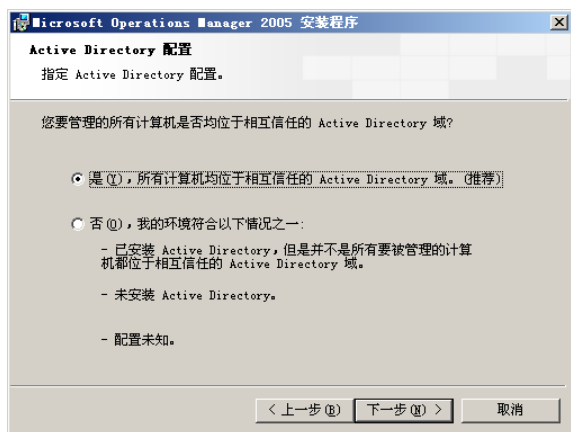


图 18-17 “Active Directory 配置”对话框



图 18-18 “已准备好安装”对话框

15 单击“安装”按钮，开始安装 MOM 2005，完成后显示如图 18-19 所示的“正在完成 Microsoft Operations Manager 2005 安装向导”对话框。默认选中“启动 MOM 管理员控制台”复选框，可以在安装完成后立即启动 MOM 管理控制台。

16 单击“完成”按钮，完成 Microsoft Operations Manager 2005 组件的安装，并自动打开“MOM 2005 管理员控制台”窗口，如图 18-20 所示。也可以单击“开始”→“所有程序”→“Microsoft Operations Manager 2005”→“MOM 2005 管理员控制台”选项，打开 MOM 2005 管理员控制台。



图 18-19 “正在完成 Microsoft Operations Manager 2005 安装向导”对话框

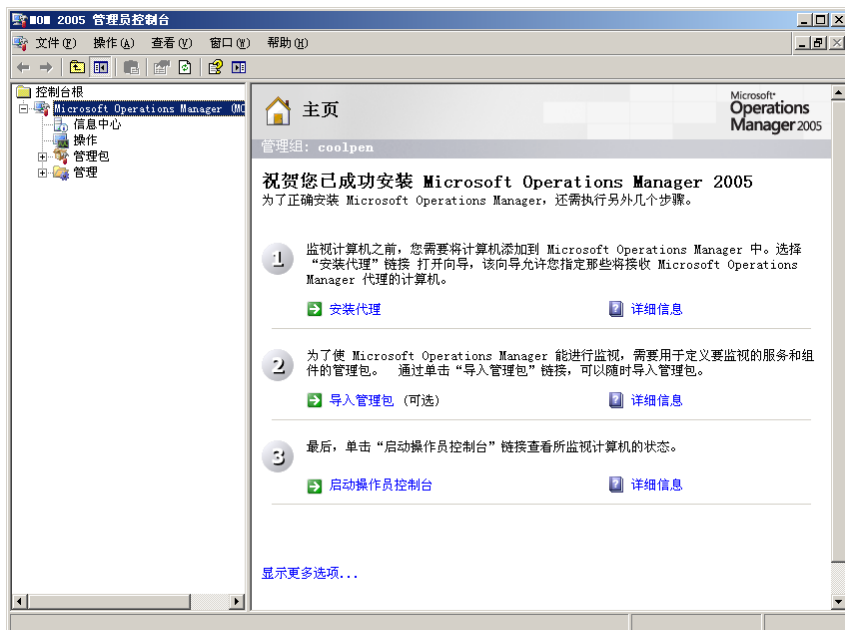


图 18-20 “MOM 2005 管理员控制台”窗口

18.2.3 安装 Microsoft Operations Manager 2005 报表

① 在“Microsoft Operations Manager 2005 安装程序资源”对话框中单击“安装 Microsoft Operations Manager 2005 报表”超级链接，启动报表安装向导，如图 18-21 所示。



图 18-21 报表安装向导

② 单击“下一步”按钮，显示如图 18-22 所示的“最终用户许可协议”对话框，选择“我接受许可协议中的条款”单选按钮。

③ 单击“下一步”按钮，显示如图 18-23 所示的“注册信息”对话框，分别在“用户名”和“单位”文本框中键入用户名和单位名称即可。



图 18-22 “最终用户许可协议”对话框

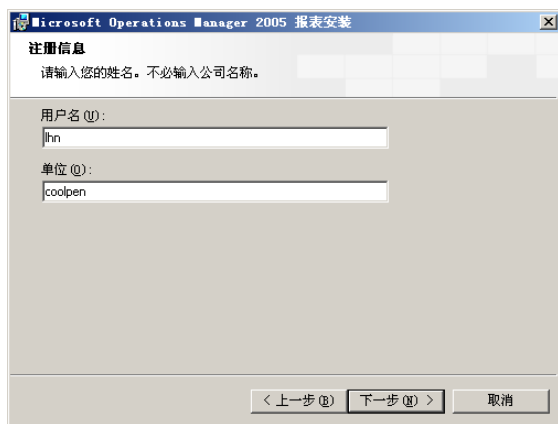


图 18-23 “注册信息”对话框

④ 单击“下一步”按钮，显示如图 18-24 所示的“目标文件夹”对话框，用于设置安装路径。

⑤ 单击“下一步”按钮，显示如图 18-25 所示的“SQL Server 报表服务服务器”对话框。清除“自动检查虚拟目录”复选框，并在“报表服务器虚拟目录”文本框中输入“reportserver”，在“报表管理器虚拟目录”文本框中输入“reports”。



图 18-24 “目标文件夹”对话框

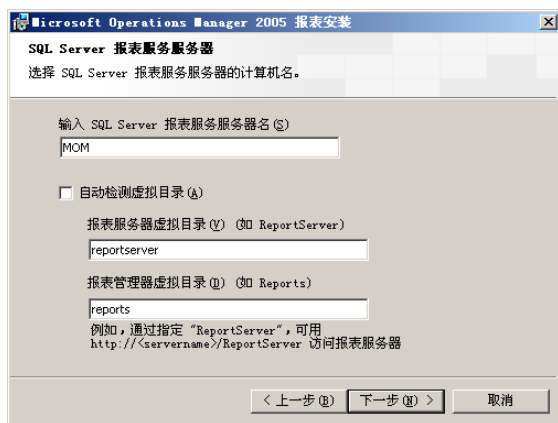


图 18-25 “SQL Server 报表服务服务器”对话框

提示

此处的两个虚拟目录是 SQL Server 2005 在 IIS 中创建的，如图 18-26 所示。

⑥ 单击“下一步”按钮，显示如图 18-27 所示的“已通过先决条件检查”对话框。

⑦ 单击“下一步”按钮，显示如图 18-28 所示的“MOM 数据库服务器实例”对话框，在“MOM 数据库服务器”文本框中键入 MOM 数据库服务器名称。

⑧ 单击“下一步”按钮，显示如图 18-29 所示的“SQL Server 数据库实例”对话框，在“SQL Server 实例”下拉列表框中选择数据库实例。

⑨ 单击“下一步”按钮，显示如图 18-30 所示的“数据库和日志文件信息”对话框，设置数据库大小及位置。

⑩ 单击“下一步”按钮，显示如图 18-31 所示的“数据库传送任务账户”对话框，在其中指定可以同时访问 MOM 数据库和报表数据库的域账户。

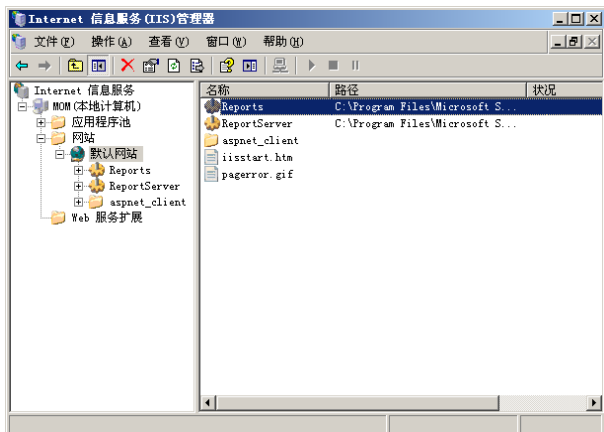


图 18-26 SQL Server 2005 在 IIS 中创建的两个虚拟目录

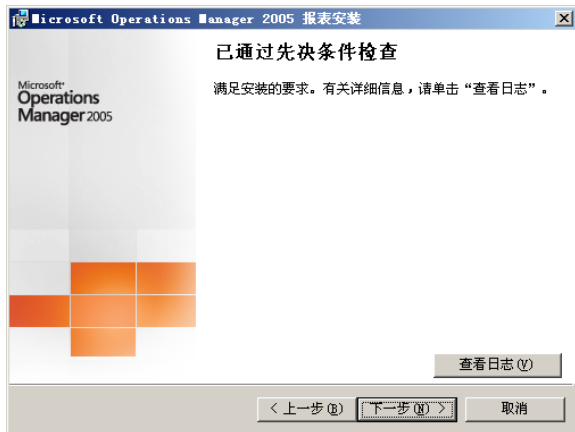


图 18-27 “已通过先决条件检查”对话框



图 18-28 “MOM 数据库服务器实例”对话框

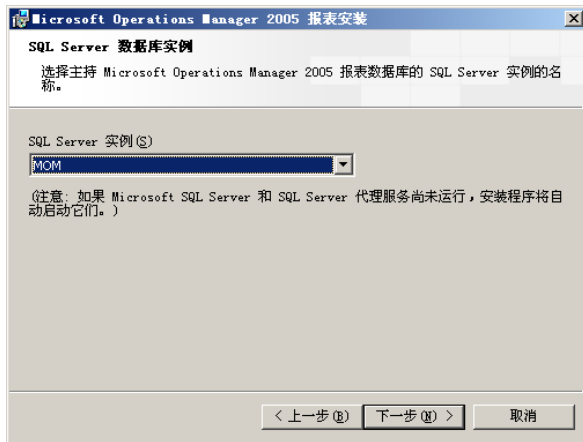


图 18-29 “SQL Server 数据库实例”对话框

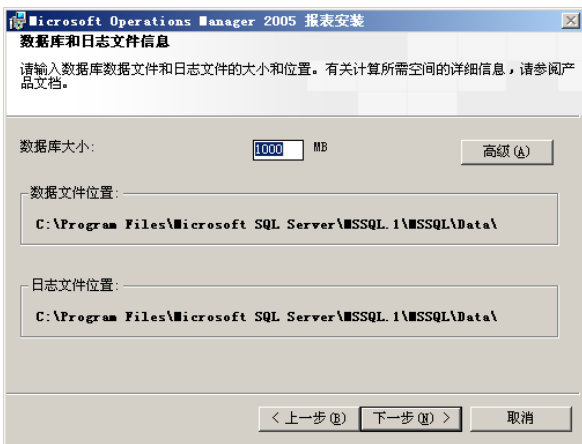


图 18-30 “数据库和日志文件信息”对话框

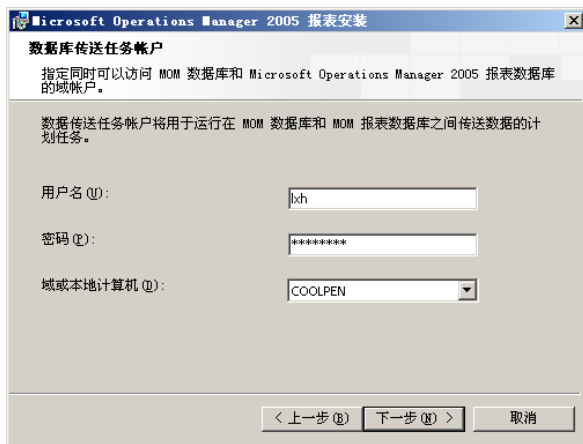


图 18-31 “数据库传送任务账户”对话框

⑪ 单击“下一步”按钮，显示如图 18-32 所示的“报表用户账户”对话框，在其中指定 MOM 报表服务器连接到 MOM 报表数据库时使用的账户。需要注意的是，此处的报表用户账户不能与数据库传送任务的账户相同。

⑫ 单击“下一步”按钮，显示如图 18-33 所示的“操作数据报告设置”对话框，在其中选择是否发送操作报告。

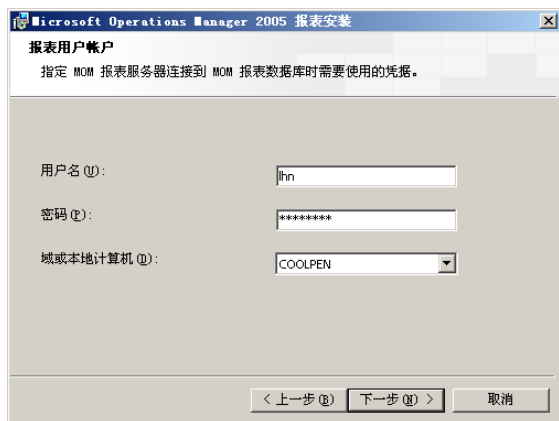


图 18-32 “报表用户账户”对话框

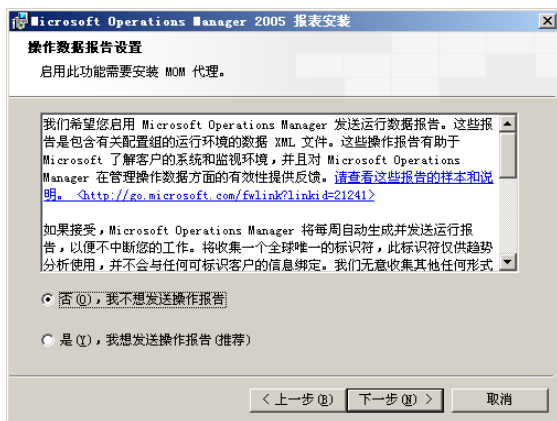


图 18-33 “操作数据报告设置”对话框

⑬ 单击“下一步”按钮，显示如图 18-34 所示的“已准备好安装”对话框，提示安装向导已准备好。

⑭ 单击“下一步”按钮，显示如图 18-35 所示的“正在完成 Microsoft Operations Manager 2005 报表安装向导”对话框。

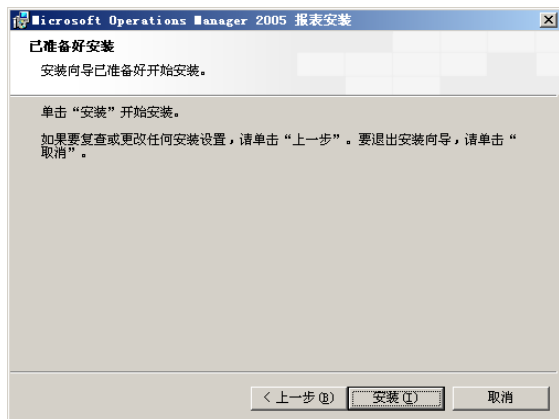


图 18-34 “已准备好安装”对话框



图 18-35 “正在完成 Microsoft Operations Manager 2005 报表安装向导”对话框

⑮ 单击“完成”按钮，MOM 2005 报表安装完成。

18.3 安装代理

为了使 MOM 2005 能够监控网络中的服务器，必须首先将计算机添加到 MOM 中。可以在 MOM 2005 中先发现网络中的服务器，然后利用“代理安装向导”在服务器上安装代理程序即可。

18.3.1 计算机发现规则

在 MOM 2005 中，所监控的客户端就是网络中的服务器。因此在安装完成 MOM 2005 后需要先设置计算机规则，以发现客户端计算机，从而实现监控。

① 打开如图 18-36 所示的“MOM 2005 管理员控制台”窗口，依次展开“Microsoft Operations Manager”→“管理”→“计算机”→“计算机发现规则”选项。

② 右击“计算机发现规则”选项，在快捷菜单中选择“创建计算机发现规则”选项，显示如图 18-37 所示的“计算机发现规则”对话框。

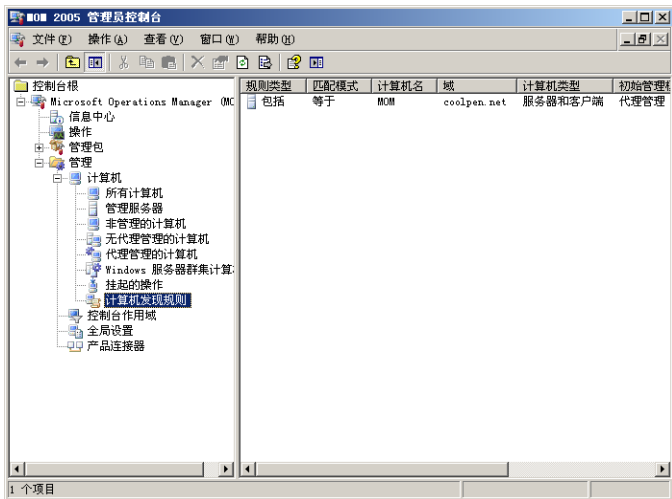


图 18-36 “MOM 2005 管理员控制台”窗口

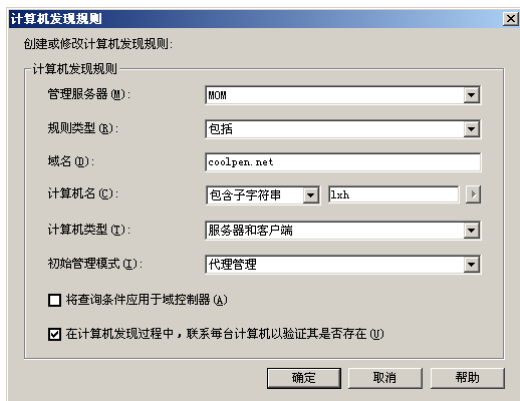


图 18-37 “计算机发现规则”对话框

③ 在“规则类型”下拉列表框中选择“包括”选项。在“域名”文本框中键入 Active Directory 域名，如 coolpen.net。在“计算机名”下拉列表框中选择“包含子字符串”选项，在右侧的文本框中键入包含的字符串。在“计算机类型”下拉列表框中选择“服务器和客户端”选项，在“初始管理模式”下拉列表框中选择“代理管理”选项。

④ 单击“确定”按钮，创建完成规则。为了能够发现网络中的所有服务器，应创建多个规则，如图 18-38 所示。

⑤ 右击“计算机发现规则”选项，在快捷菜单中选择“立即运行计算机发现”命令，显示如图 18-39 所示的“Microsoft Operations Manager”提示框。提示计算机发现任务已提交给管理服务器，单击“确定”按钮即可。

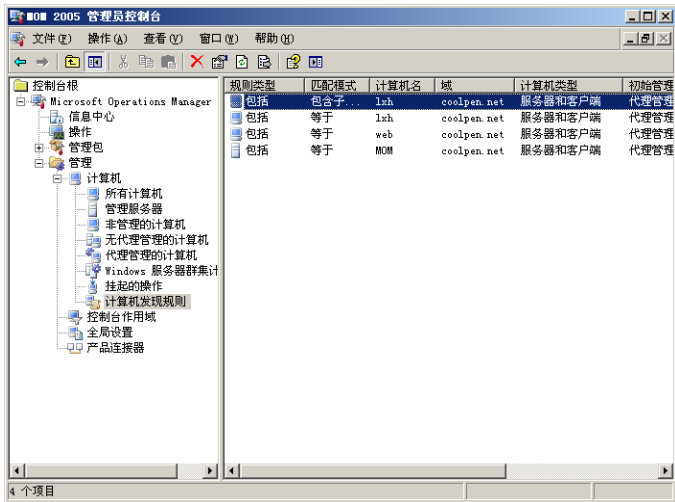


图 18-38 创建多个规则



图 18-39 “Microsoft Operations Manager”提示框

⑥ 在“MOM 2005 管理员控制台”窗口中单击左窗格中的“所有计算机”选项，即可看到所发现的所有计算机，如图 18-40 所示。

提示 如果没有显示发现的计算机，可再次选择“立即运行计算机规则发现”选项，并刷新。

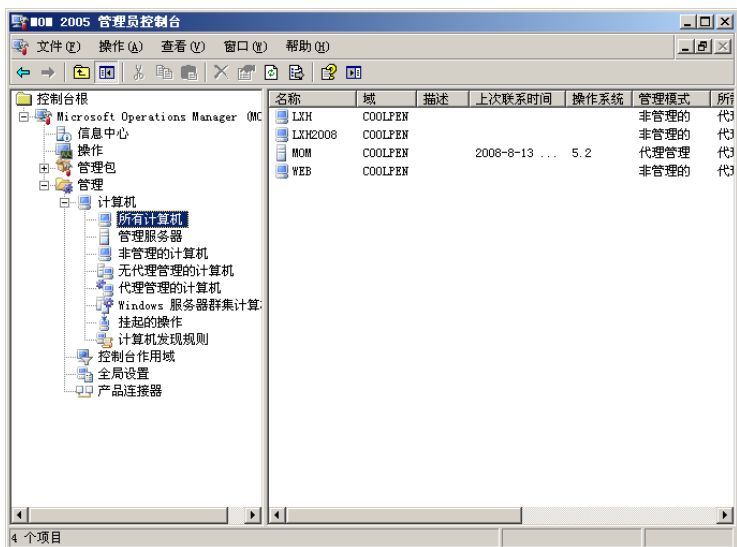


图 18-40 已发现的计算机

18.3.2 安装代理服务

客户端发现成功后，直接在 MOM 服务器上就可以在已发现的服务器中安装代理服务。不过若要成功安装代理，必须拒绝挂起的操作。

① 在如图 18-41 所示的“MOM 2005 管理员控制台”窗口中选择“挂起的操作”选项，选择服务器名。右击并选择快捷菜单中的“拒绝挂起的安装”选项，将其拒绝即可。

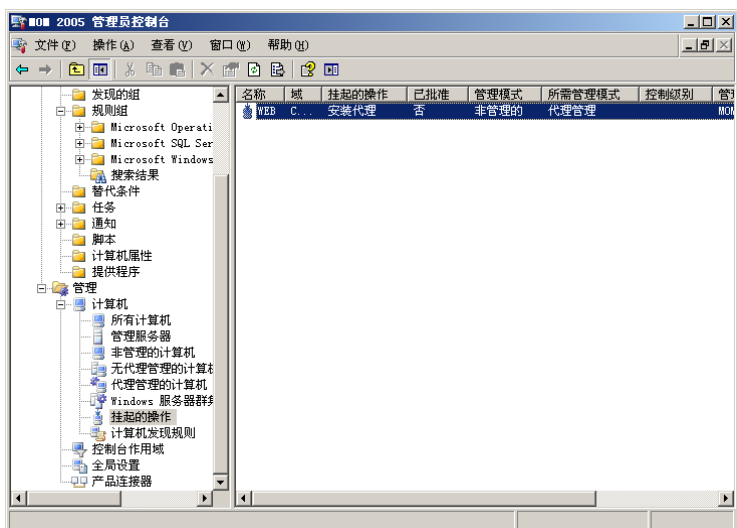


图 18-41 “MOM 2005 管理员控制台”窗口

② 在“MOM 2005 管理员控制台”窗口中单击“安装代理”超级链接，打开“安装/卸载代理向导”对话框，如图 18-42 所示。



提示

展开“管理”→“计算机”，右击“所有计算机”并选择快捷菜单中的“安装/卸载代理向导”选项，也可以启动“安装/卸载代理向导”。

③ 单击“下一步”按钮，显示如图 18-43 所示的“发现计算机和安装代理的方法”对话框，选择“浏览或键入特定计算机名”单选按钮。

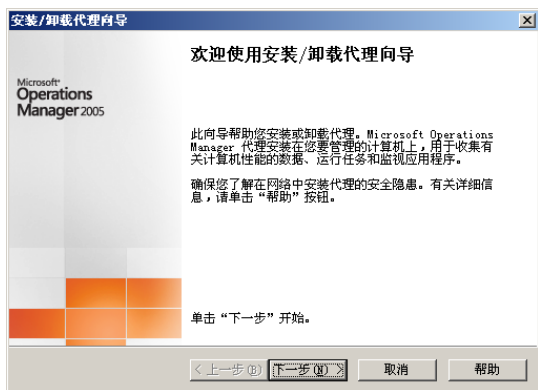


图 18-42 “欢迎使用安装/卸载代理向导”对话框

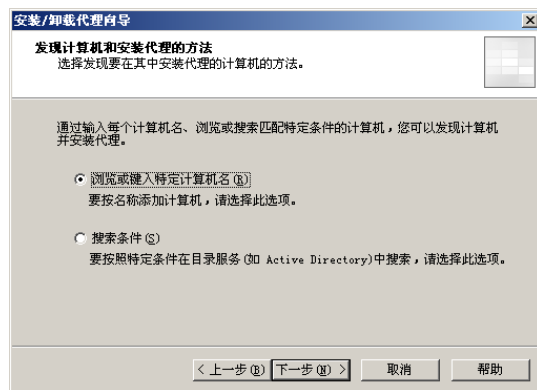


图 18-43 “发现计算机和安装代理的方法”对话框

- ④ 单击“下一步”按钮，显示如图 18-44 所示的“计算机名”对话框。
- ⑤ 单击“浏览”按钮，显示如图 18-45 所示的“选择计算机”对话框。单击“高级”按钮。然后单击“立即查找”按钮，在“搜索结果”列表框中选择需要安装代理的计算机。

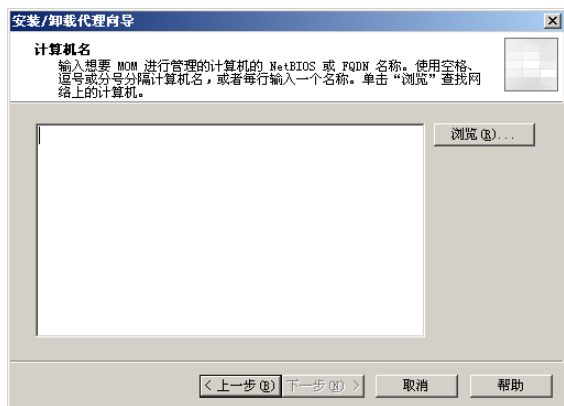


图 18-44 “计算机名”对话框

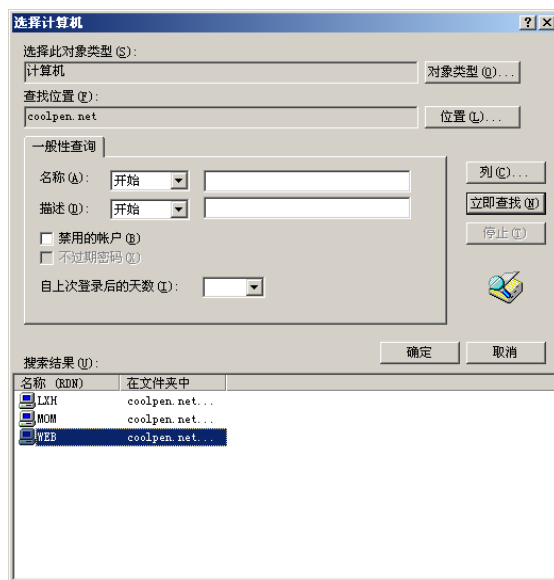


图 18-45 “选择计算机”对话框

- ⑥ 依次单击“确定”按钮返回，即可看到已添加的计算机，如图 18-46 所示。
- ⑦ 单击“下一步”按钮，显示如图 18-47 所示的“代理安装权限”对话框，在其中选择“其他”单选按钮并键入用户名。

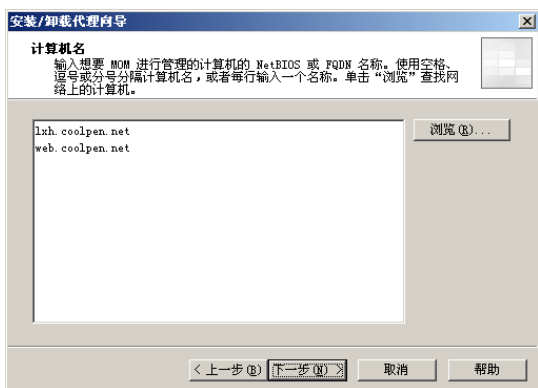


图 18-46 已添加的计算机

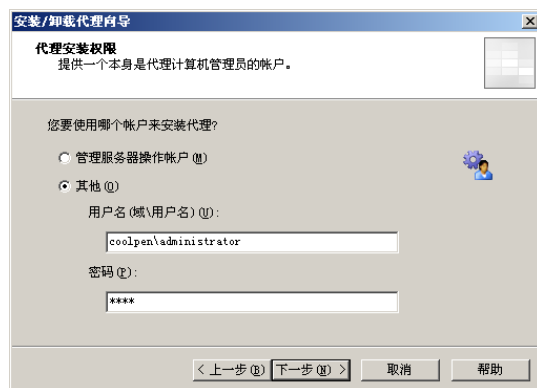


图 18-47 “代理安装权限”对话框

⑧ 单击“下一步”按钮，显示如图 18-48 所示的“代理操作账户”对话框，在其中选择“其他”单选按钮并键入用户名。

⑨ 单击“下一步”按钮，显示如图 18-49 所示的“代理安装目录”对话框，保留默认值即可。

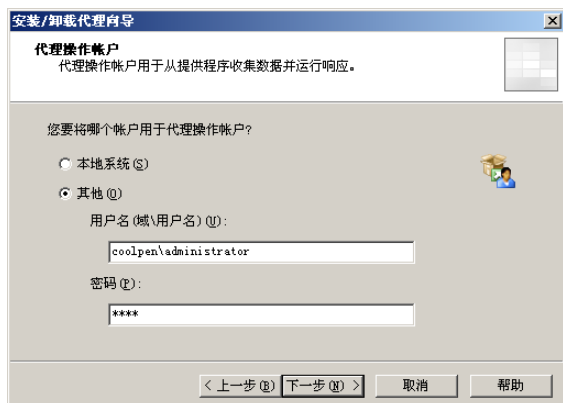


图 18-48 “代理操作账户”对话框

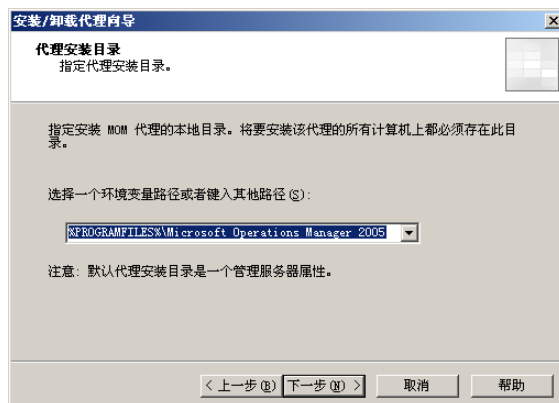


图 18-49 “代理安装目录”对话框

⑩ 单击“下一步”按钮，显示如图 18-50 所示的“正在完成安装/卸载代理向导”对话框。

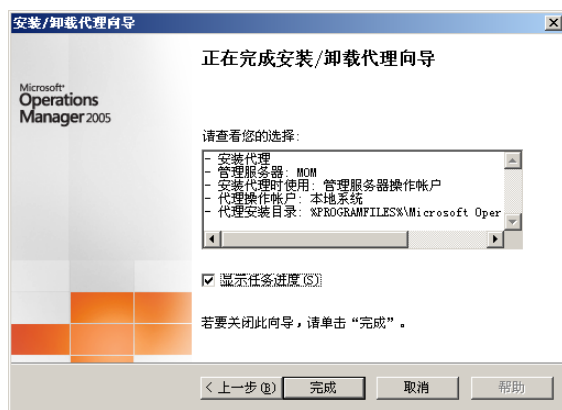


图 18-50 “正在完成安装/卸载代理向导”对话框

⑪ 单击“完成”按钮，显示如图 18-51 所示的“Microsoft Operations Manager 任务进度”对话框，开始自动执行安装任务。安装完成后单击“详细信息”按钮，可以看到已安装成功的计算机。



图 18-51 “Microsoft Operations Manager 任务进度”对话框

**提示**

如果某个计算机安装失败，可选择该计算机名，在“所选计算机的详细资料”列表框中可以看到安装失败的原因。

⑫ 单击“关闭”按钮关闭，代理服务安装完成。在“代理管理的计算机”窗口中即可看到成功安装的代理计算机，如图 18-52 所示。

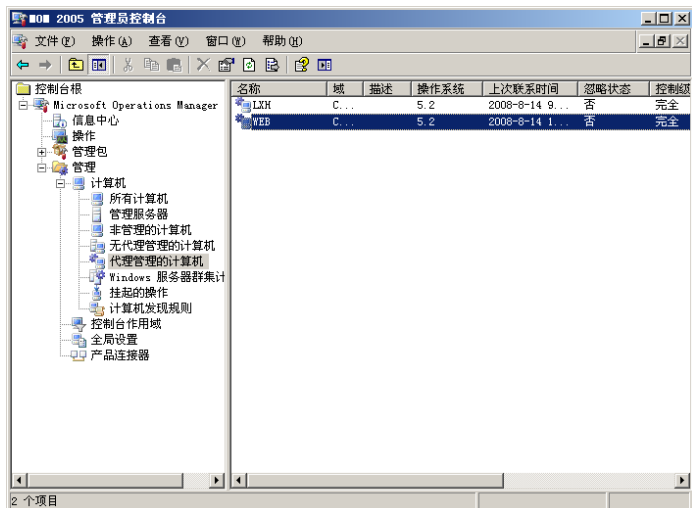


图 18-52 成功安装的代理计算机

18.4 安装管理包

MOM 2005 监控网络服务是通过相应的管理包来实现的，如果要监控某种服务，必须首先安装相应的组件。这些监控组件既可以从 MOM 安装光盘中获得，也可以从微软网站下载。

18.4.1 下载管理包

微软网站提供了多个 MOM 管理包以供下载，将下载的管理包导入到 MOM 管理服务器中即可。需要注意的是，下载的管理包格式为 MSI，应首先将管理包安装至一个临时目录下，然后导入管理包。

① 打开“MOM 2005 管理员控制台”窗口，在左窗格中选“信息中心”选项，显示如图 18-53 所示的“信息中心”窗口。



图 18-53 “信息中心”窗口

② 单击“下载和更新”超级链接，显示如图 18-54 所示的“Downloads for Microsoft Operations Manager 2005”窗口。

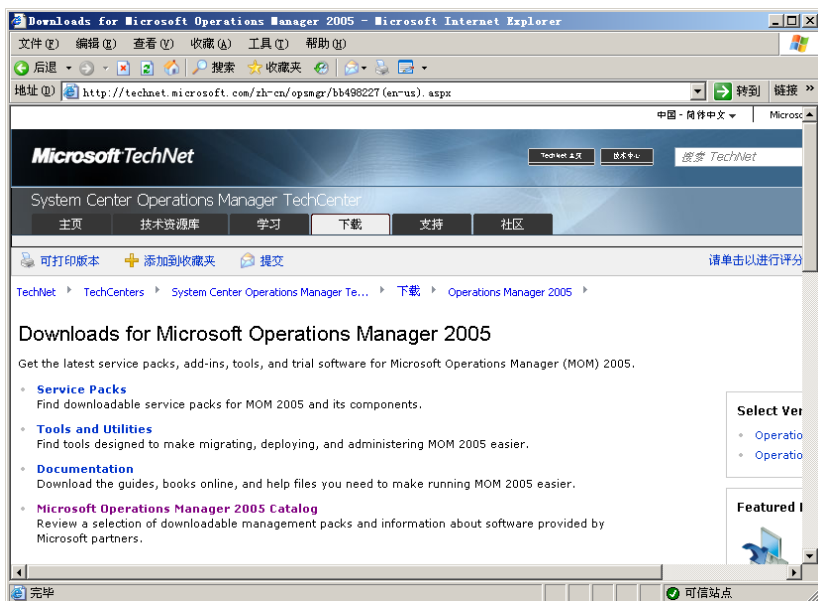


图 18-54 “Downloads for Microsoft Operations Manager 2005”窗口

③ 单击“Microsoft Operations Manager 2005 Catalog”超级链接，显示如图 18-55 所示的“Management Pack and product Connector Catalog”窗口。

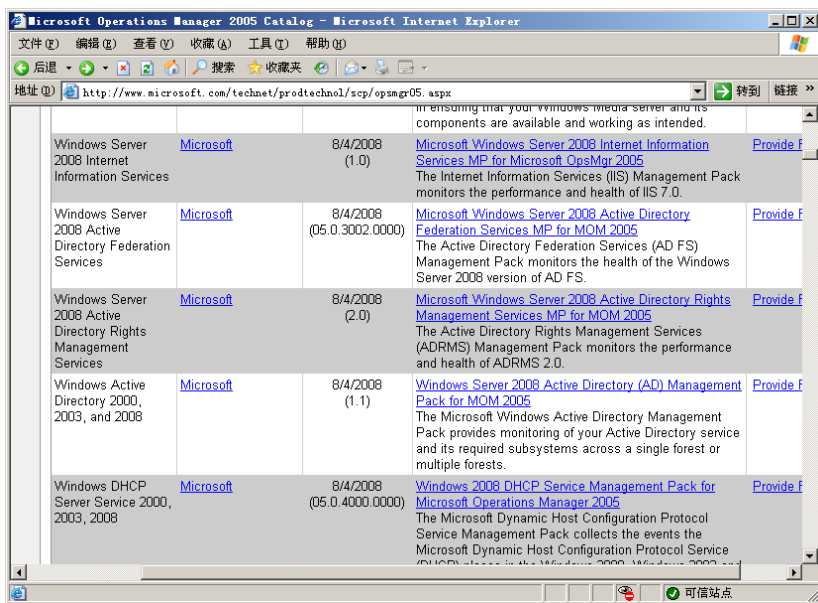


图 18-55 “Management Pack and product Connector Catalog”窗口

④ 找到要下载的管理包，例如“Windows Active Directory 2000,2003, and 2008”。单击“Windows Server 2008 Active Directory (AD) Management Pack for MOM 2005”超级链接，显示如图 18-56 所示的下载窗口。

⑤ 单击“Download”按钮，即可下载选择的管理包。下载完成后运行下载的 MSI 文件，显示如图 18-57 所示的“License Agreement”对话框，选择“I Agree”单选按钮。

⑥ 单击“Next”按钮，显示如图 18-58 所示的“Select Installation Folder”对话框。单击“Browse”按钮，可以选择要解压到的目录。



图 18-56 下载窗口

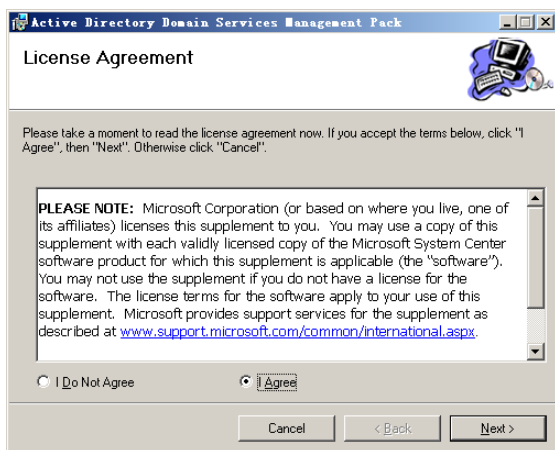


图 18-57 “License Agreement” 对话框

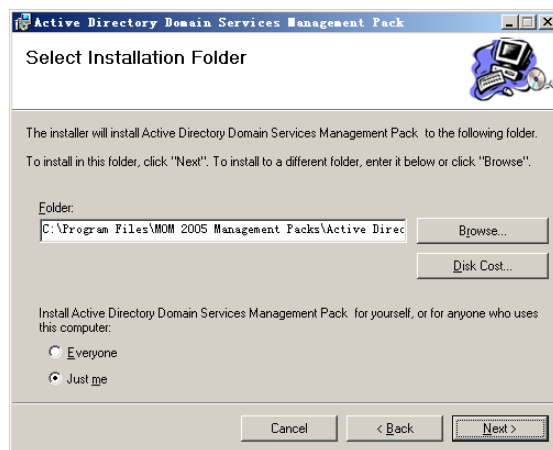


图 18-58 “Select Installation Folder” 对话框

- ⑦ 单击“Next”按钮，显示如图 18-59 所示的“Confirm Installation”对话框。
- ⑧ 单击“Next”按钮，开始解压缩管理包，完成后显示如图 18-60 所示的“Installation Complete”对话框。

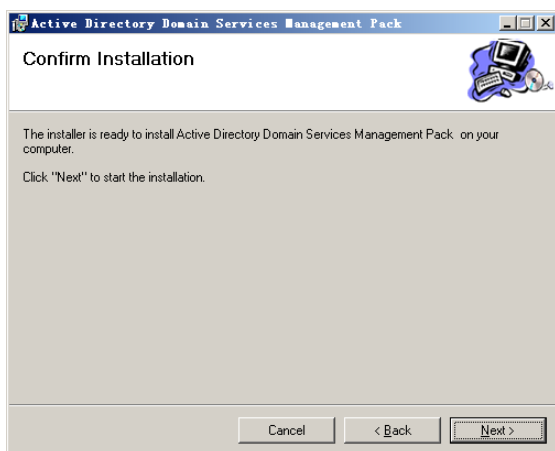


图 18-59 “Confirm Installation” 对话框

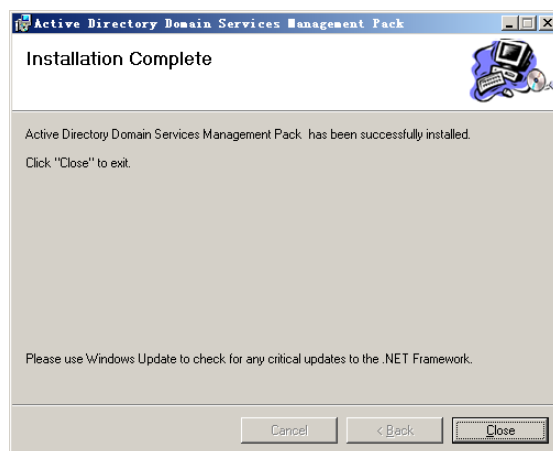


图 18-60 “Installation Complete” 对话框

- ⑨ 单击“Close”按钮完成操作，按照同样操作可下载并解压缩其他管理包。

18.4.2 导入 Active Directory 管理包

导入 Active Directory 管理包的操作步骤如下。

- ① 在“MOM 2005 管理员控制台”窗口中选择“管理包”选项，显示如图 18-61 所示的“管理包”窗口。



图 18-61 “管理包”窗口

- ② 单击“导入/导出管理包”超级链接，打开“管理包导入/导出向导”对话框，如图 18-62 所示。

- ③ 单击“下一步”按钮，显示如图 18-63 所示的“导入或导出管理包”对话框，选择“导入管理包和/或报表”单选按钮。

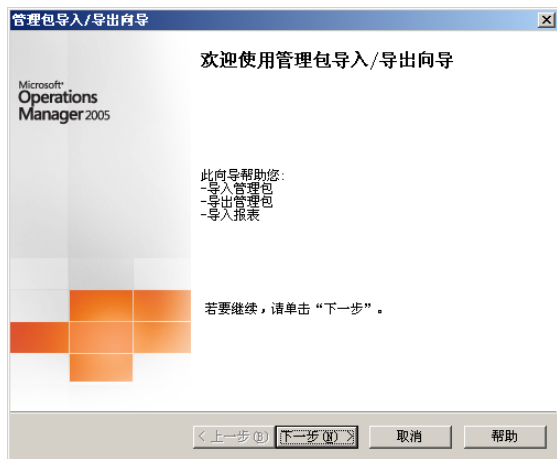


图 18-62 “管理包导入/导出向导”对话框

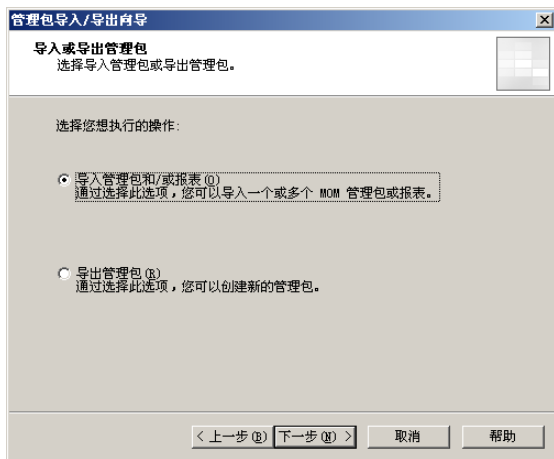


图 18-63 “导入或导出管理包”对话框

- ④ 单击“下一步”按钮，显示如图 18-64 所示的“选择文件夹，再选择导入类型”对话框。单击“浏览”按钮，指定管理包所在的文件夹，在“导入类型”选项组中选择“仅导入管理包”单选按钮。

- ⑤ 单击“下一步”按钮，显示如图 18-65 所示的“选择管理包”对话框。在“请选择一个或多个要导入的管理包”列表框中选择 Active Directory 管理包，在“导入选项”选项组中选择“更新现有管理包。保留自定义规则、启用/禁用设置和公司知识”单选按钮。选中“备份现有管理包”复选框，管理包默认备份到“C:\Program Files\Microsoft Operations Manager 2005\MPBackup\”目录。

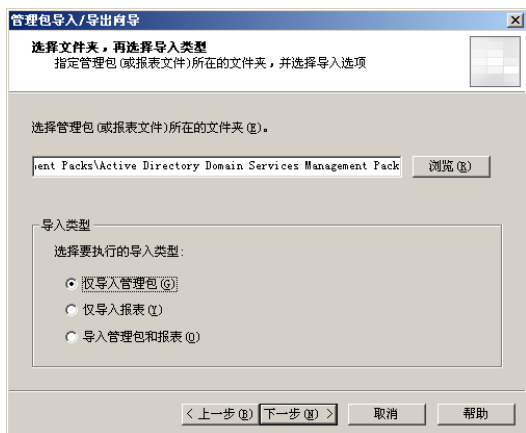


图 18-64 “选择文件夹，再选择导入类型”对话框



图 18-65 “选择管理包”对话框

⑥ 单击“下一步”按钮，显示如图 18-66 所示的“正在完成导入/导出向导”对话框。

⑦ 单击“完成”按钮，开始执行管理包导入进程。导入完成后，显示如图 18-67 所示的“导入状态”对话框。

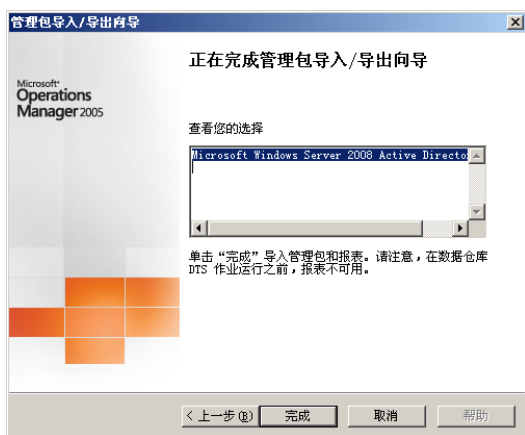


图 18-66 “正在完成导入/导出向导”对话框

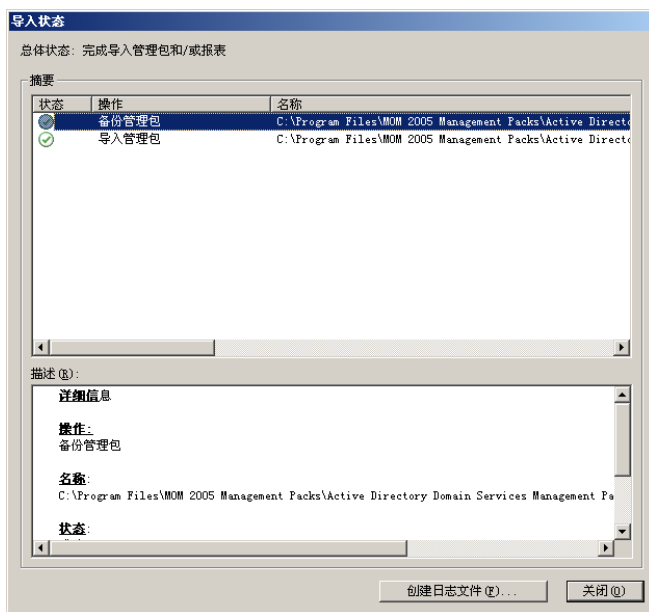


图 18-67 “导入状态”对话框

⑧ 单击“关闭”按钮，关闭“管理包导入/导出向导”。在“MOM 2005 管理员控制台”窗口中右击“管理包”选项，选择快捷菜单中的“提交配置更改”选项，显示如图 18-68 所示的“配置更改”对话框。

⑨ 单击“关闭”按钮关闭即可。

18.4.3 导入 Microsoft SQL Server 管理包

将 SQL Server 管理包下载以后，即可导入到 MOM 2005 中。其导入过程和导入 Active Directory 管理包的过程完全相同，此处不再赘述。

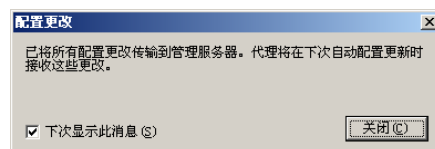


图 18-68 “配置更改”对话框

18.5 计算机组

在 MOM 2005 中为了顺利监控目标服务器，应创建计算机组，并将服务器添加到计算机组中。这

样，在操作员控制台中才可以监控到服务器产生的事件、警报和性能规则。

18.5.1 创建自定义组

创建自定义组的操作步骤如下。

① 打开“管理员控制台”窗口，依次展开“Microsoft Operations Manager”→“管理包”→“计算机组”选项，显示如图 18-69 所示的“计算机组”窗口。默认情况下，MOM 2005 已经内置一些计算机组。

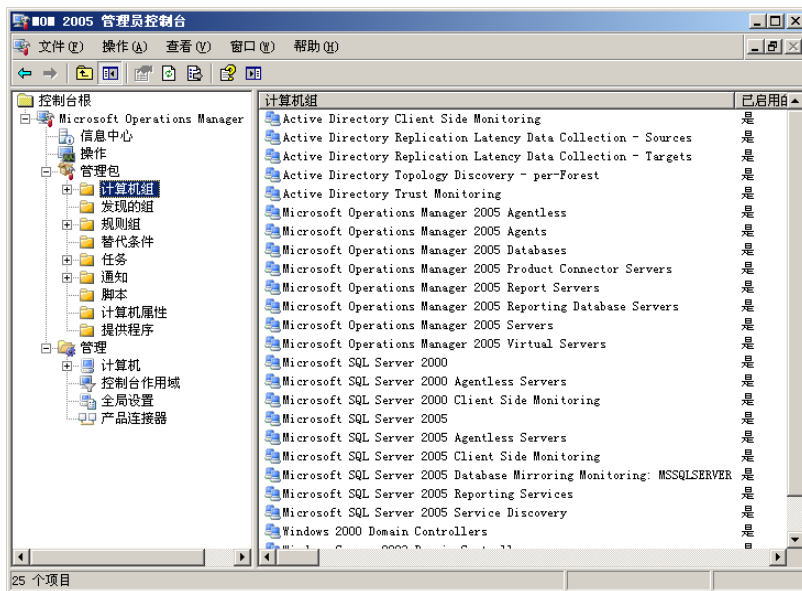


图 18-69 “计算机组”窗口

② 右击“计算机组”选项，在快捷菜单中选择“创建计算机组”选项，显示如图 18-70 所示的“欢迎使用创建计算机组向导”对话框。

③ 单击“下一步”按钮，显示如图 18-71 所示的“常规”对话框。在“名称”文本框中键入新计算机组的名称，在“描述”文本框中键入该计算机组的说明。

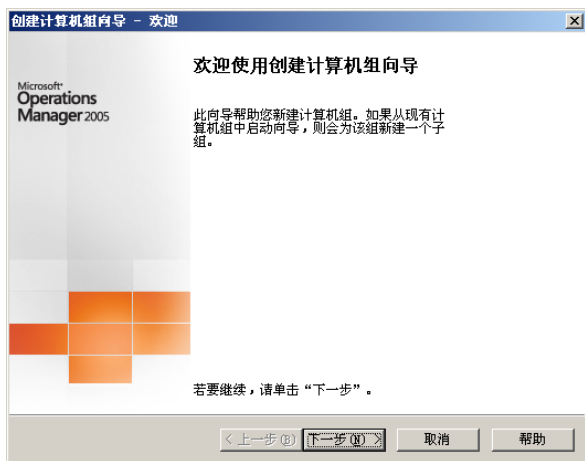


图 18-70 “欢迎使用创建计算机组向导”对话框

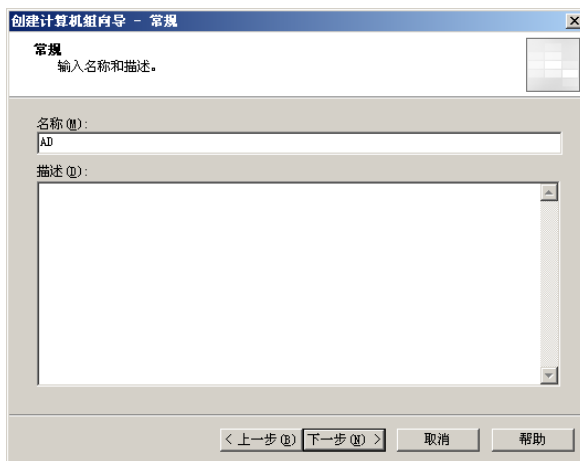


图 18-71 “常规”对话框

④ 单击“下一步”按钮，显示如图 18-72 所示的“包括的子组”对话框。

⑤ 单击“添加”按钮，显示如图 18-73 所示的“添加子组”对话框，在“选择要添加的一个或多个计算机组”列表框中选择需要添加的计算机组。

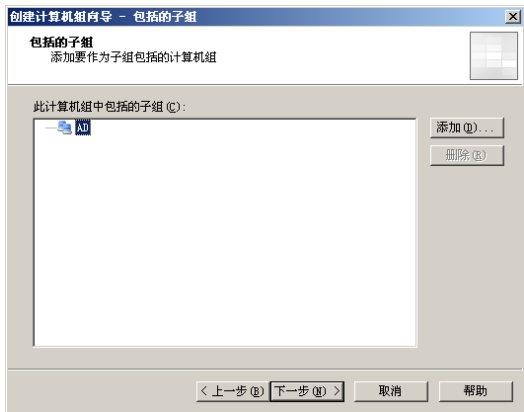


图 18-72 “包括的子组”对话框



图 18-73 “添加子组”对话框

⑥ 单击“确定”按钮添加，并返回“包括的子组”对话框。单击计算机组左侧的“+”按钮，显示添加的计算机子组，如图 18-74 所示。

⑦ 单击“下一步”按钮，显示如图 18-75 所示的“包括的计算机”对话框。

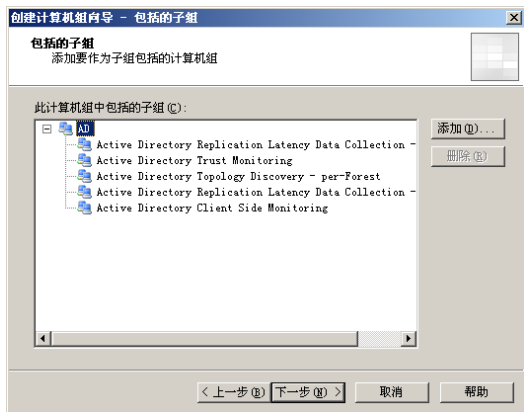


图 18-74 添加的计算机子组

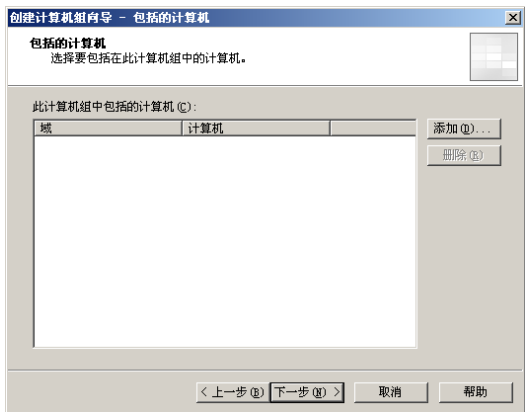


图 18-75 “包括的计算机”对话框

⑧ 单击“添加”按钮，显示如图 18-76 所示的“添加计算机”对话框。展开域名“COOLPEN”，显示可用的计算机名称列表，选中要包含在该计算机组中的计算机。

⑨ 单击“确定”按钮，关闭“添加计算机”对话框，返回到如图 18-77 所示的“包括的计算机”对话框，所添加的计算机即可显示在列表框中。

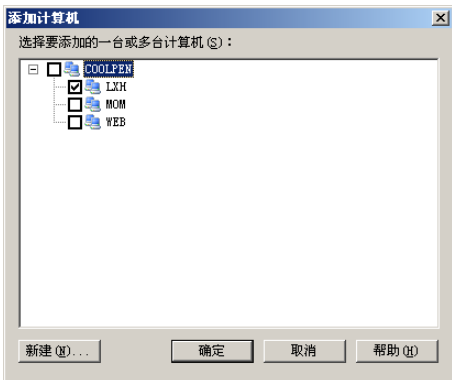


图 18-76 “添加计算机”对话框



图 18-77 “包括的计算机”对话框

⑩ 单击“下一步”按钮，显示如图 18-78 所示的“排除的计算机”对话框，可以添加要从该计算机组中删除的计算机。

⑪ 单击“下一步”按钮，显示如图 18-79 所示的“搜索计算机”对话框。在其中指定搜索计算机的条件，此处保留默认值即可。

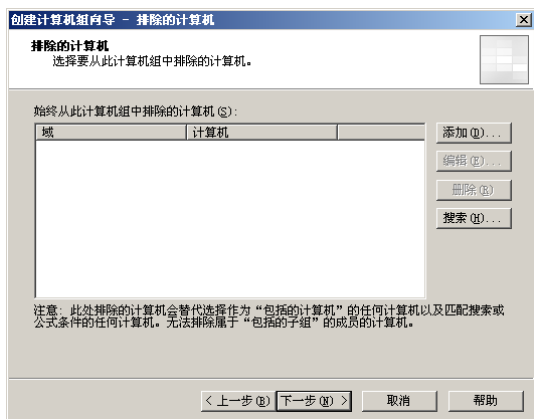


图 18-78 “排除的计算机”对话框

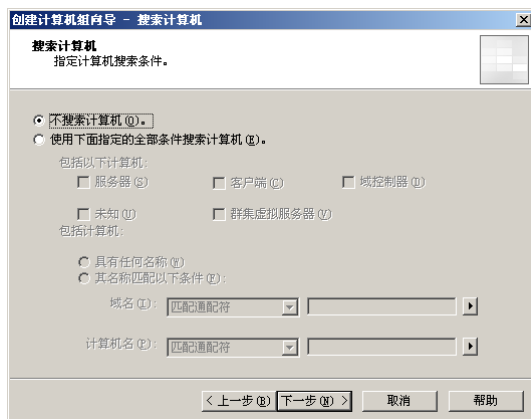


图 18-79 “搜索计算机”对话框

⑫ 单击“下一步”按钮，显示如图 18-80 所示的“公式”对话框，保留默认值即可。

⑬ 单击“下一步”按钮，显示如图 18-81 所示的“状态汇总策略”对话框，在其中选择默认的“任何成员计算机或子组的最差状态”单选按钮即可。

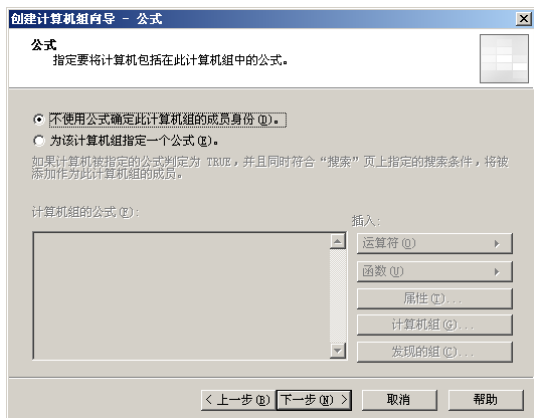


图 18-80 “公式”对话框

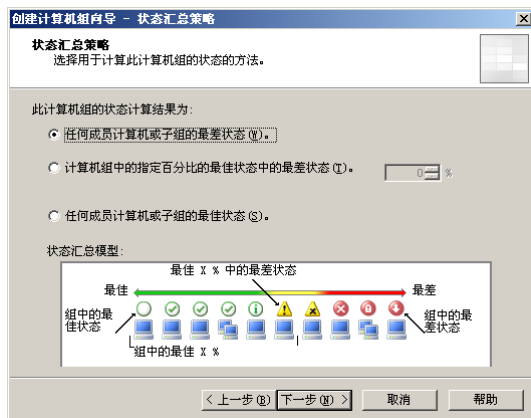


图 18-81 “状态汇总策略”对话框

⑭ 单击“下一步”按钮，显示如图 18-82 所示的“确认”对话框，其中显示前面所做的配置。如果需要修改，可单击“上一步”按钮返回。

⑮ 单击“下一步”按钮，显示如图 18-83 所示的“正在完成创建计算机组向导”对话框。



图 18-82 “确认”对话框

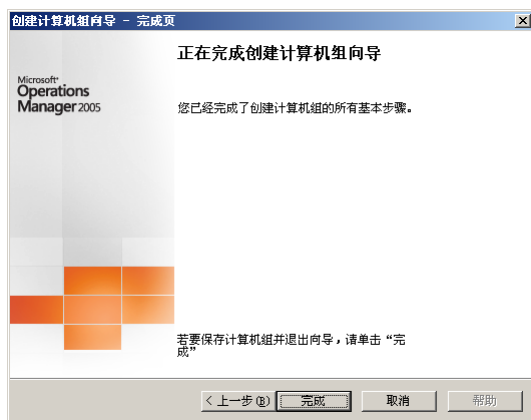


图 18-83 “正在完成创建计算机组向导”对话框

- ⑫ 单击“完成”按钮，关闭“创建计算机组向导”，计算机组创建完成。

18.5.2 设置计算机组成员

在“计算机组”窗口中默认创建了一些组，管理员也可以直接修改相应的组，添加计算机组和成员。

- ① 选择一个计算机组，例如“Microsoft SQL Server 2005”。右击并选择快捷菜单中的“属性”选项，显示如图 18-84 所示的“Microsoft SQL Server 2005 属性”对话框。

- ② 打开“包括的子组”选项卡，单击“添加”按钮。显示如图 18-85 所示的“添加子组”对话框，可以在该计算机组中添加子组。

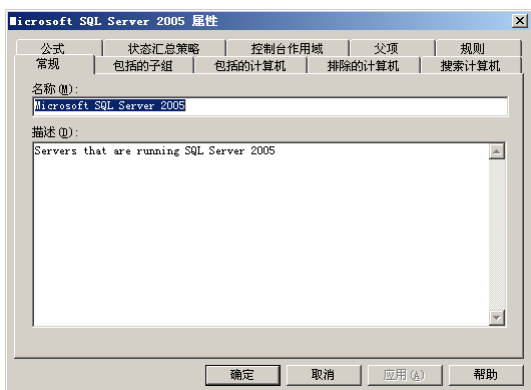


图 18-84 “Microsoft SQL Server 2005 属性”对话框

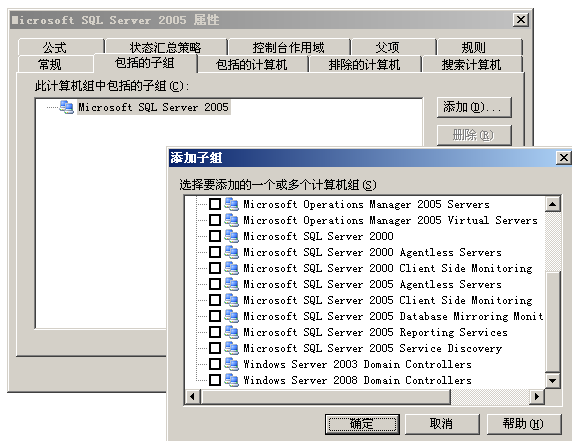


图 18-85 “添加子组”对话框

- ③ 打开“包括的计算机”选项卡，单击“添加”按钮，显示如图 18-86 所示的“添加计算机”对话框，可以在该计算机组中添加计算机。

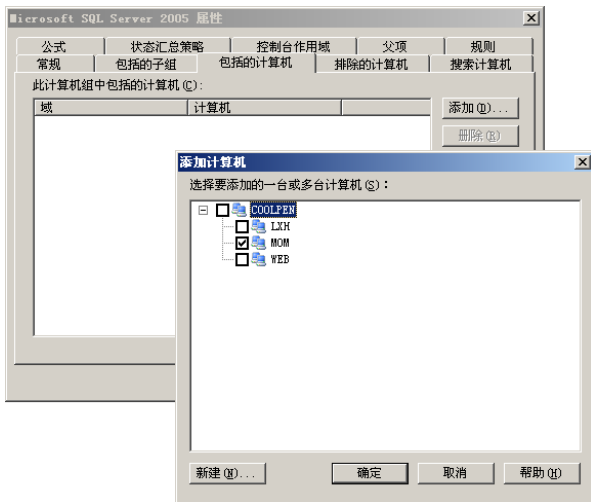


图 18-86 “添加计算机”对话框

- ④ 单击“确定”按钮，计算机组设置完成。

18.6 规则组

在每个 MOM 管理包中包含了大量的规则，包括事件规则、警报规则和性能规则。同时还提供了大量脚本，可以完成主动监控任务。网络管理员可以根据网络管理的需求创建新的规则组和新的规则。

18.6.1 创建规则组

创建规则组的操作步骤如下。

① 在“MOM 2005 管理员控制台”窗口中选择“管理包”→“规则组”选项，显示如图 18-87 所示的“规则组”窗口。

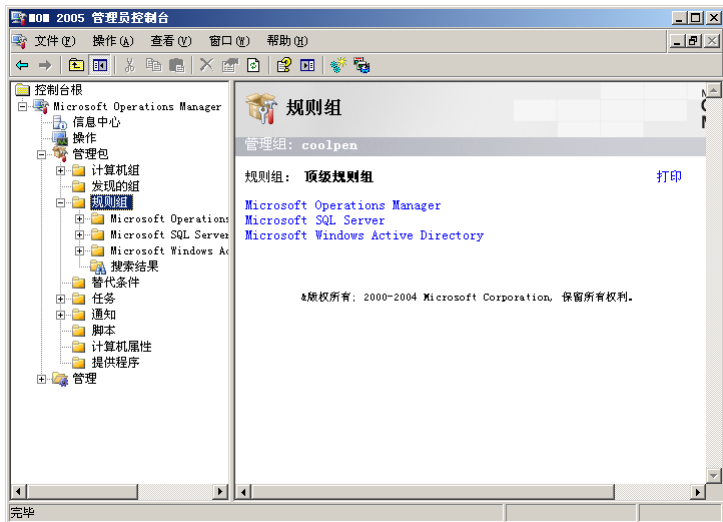


图 18-87 “规则组”窗口

② 右击“规则组”并选择快捷菜单中的“创建规则组”选项，显示如图 18-88 所示的“规则组属性-常规”对话框。在“名称”和“描述”文本框中分别键入新建的规则组的名称和描述，并选中“已启用”复选框。

③ 单击“下一步”按钮，显示如图 18-89 所示的“规则组属性-知识库”对话框。

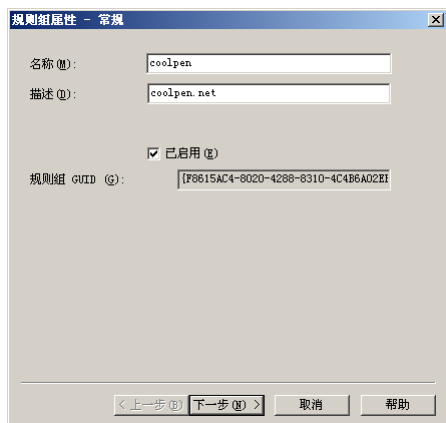


图 18-88 “规则组属性-常规”对话框



图 18-89 “规则组属性-知识库”对话框

④ 单击“编辑”按钮，显示如图 18-90 所示的“公司知识库”对话框，在文本框中可以编辑有关公司知识库的信息。

⑤ 单击“确定”按钮，关闭“公司知识库”对话框并返回“规则组属性-知识库”对话框。单击“完成”按钮，显示如图 18-91 所示的“Microsoft Operations Manager”提示框，确认是否将新规则组中的规则部署到一组计算机中。

⑥ 单击“是”按钮，显示“规则组属性”对话框。打开“计算机组”选项卡，如图 18-92 所示。

⑦ 单击“添加”按钮，显示如图 18-93 所示的“选择项目”对话框，在“计算机组”列表框中选择目标服务器组。

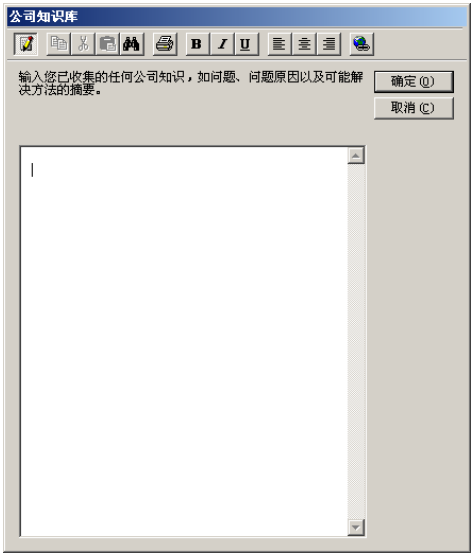


图 18-90 “公司知识库”对话框



图 18-91 “Microsoft Operations Manager”提示框

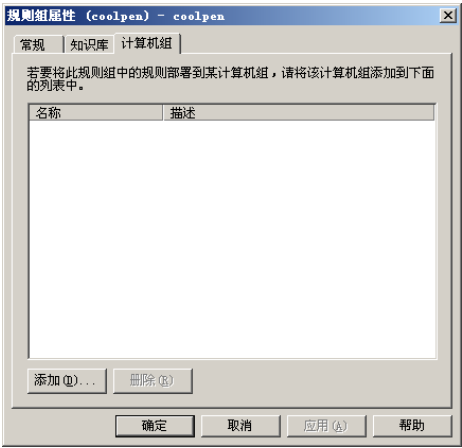


图 18-92 “计算机组”选项卡

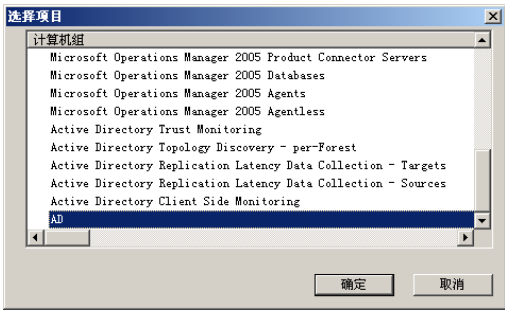


图 18-93 “选择项目”对话框

⑧ 单击“确定”按钮，将计算机组添加到列表中。单击“确定”按钮，创建完成新规则组，如图 18-94 所示。

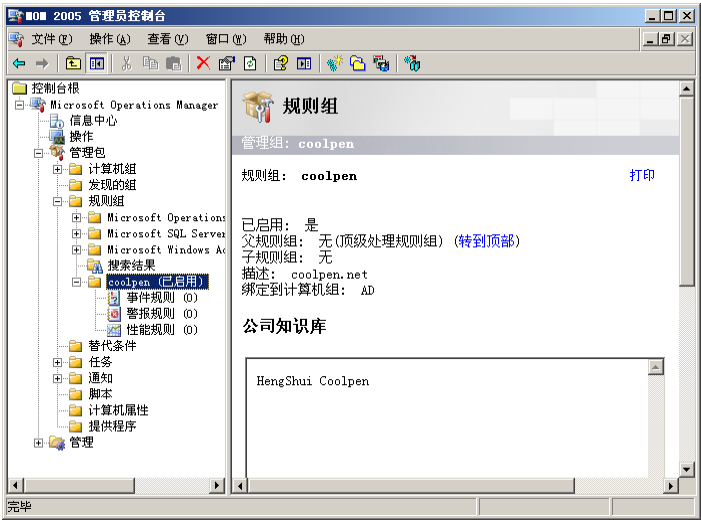


图 18-94 创建完成新规则组

新建规则组以后还没有任何规则，网络管理员可以根据网络状况自定义事件规则、警报规则和性能规则，以更加合理有效的监控网络运行状况。

18.6.2 创建事件规则

创建事件规则的操作步骤如下。

① 在“MOM 2005 管理员控制台”窗口中展开新建的规则组，选择“事件规则”选项。右击并选择快捷菜单中的“创建事件规则”选项，显示如图 18-95 所示的“选择事件规则类型”对话框。根据事件的性质选择时间的类型，以“事件警报或响应（事件）”为例说明。

② 单击“下一步”按钮，显示如图 18-96 所示的“事件规则属性-数据提供程序”对话框。在“提供程序名”列表框中选择要使用的程序，这里以“Directory Service”为例。

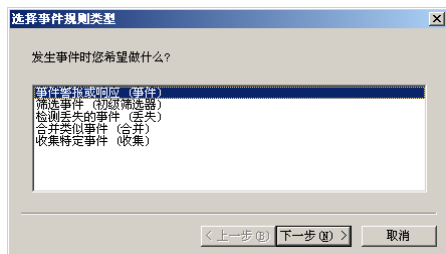


图 18-95 “选择事件规则类型”对话框



图 18-96 “事件规则属性-数据提供程序”对话框

③ 单击“下一步”按钮，显示如图 18-97 所示的“事件规则属性-条件”对话框。选择“来自源”复选框，在右侧的文本框中键入“Directory Service”。选择“具有事件 ID”复选框，键入事件编号，例如 300。选中“具有类型”复选框，在下拉列表框中选择“成功”选项。

④ 单击“下一步”按钮，显示如图 18-98 所示的“事件规则属性-计划”对话框，保留默认值即可。

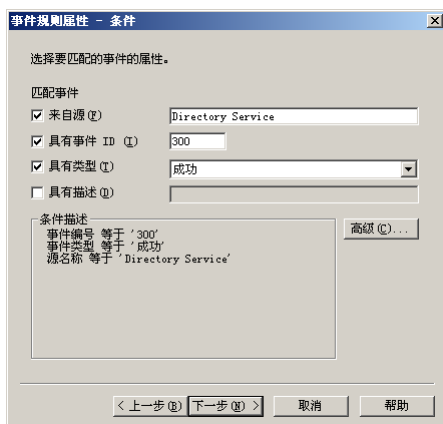


图 18-97 “事件规则属性-条件”对话框

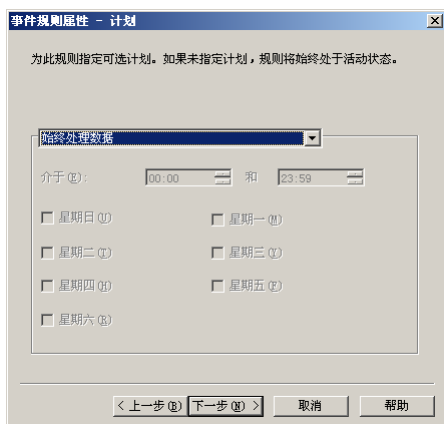


图 18-98 “事件规则属性-计划”对话框

⑤ 单击“下一步”按钮，显示如图 18-99 所示的“事件规则属性-警报”对话框。选择“生成警报”复选框，在“警报属性”选项项目中设置“警报严重性”为“错误”，设置“解决状态”为“已确认”，其他设置保留默认值。

⑥ 单击“下一步”按钮，显示如图 18-100 所示的“事件规则属性-警报抑制”对话框。选择“抑制重复警报”复选框，在“字段”下拉列表框中选择抑制警报需要的字段。

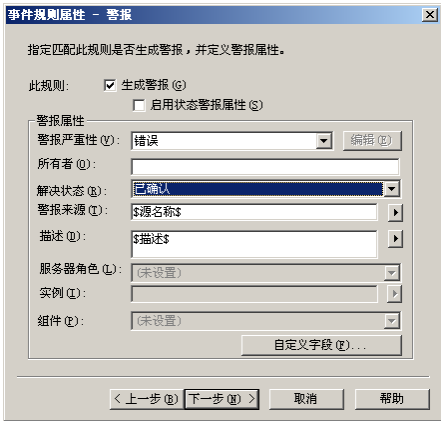


图 18-99 “事件规则属性-警报”对话框

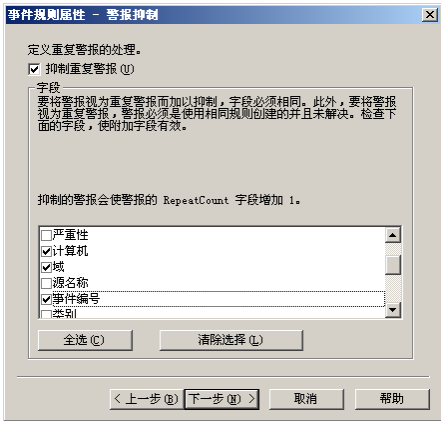


图 18-100 “事件规则属性-警报抑制”对话框

- ⑦ 单击“下一步”按钮，显示如图 18-101 所示的“事件规则属性-响应”对话框。
- ⑧ 选择“向通知组发送通知”选项，显示如图 18-102 所示的“向通知组发送通知”对话框。在“通知组”下拉列表框中选择要通知的组，此处以“Network Administrators”为例。单击“确定”按钮，返回到“事件规则属性-响应”对话框。



图 18-101 “事件规则属性-响应”对话框

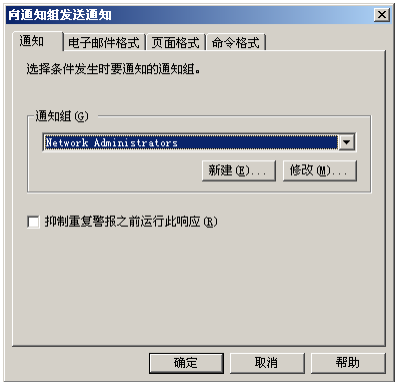


图 18-102 “向通知组发送通知”对话框

- ⑨ 单击“下一步”按钮，显示如图 18-103 所示的“事件规则属性-知识库”对话框。单击“编辑”按钮，可编辑知识库相关的文档格式以及简要说明。
- ⑩ 单击“下一步”按钮，显示如图 18-104 所示的“事件规则属性-常规”对话框。在“规则名称”文本框中键入新建规则的名称，选择“此规则已启用”复选框。



图 18-103 “事件规则属性-知识库”对话框

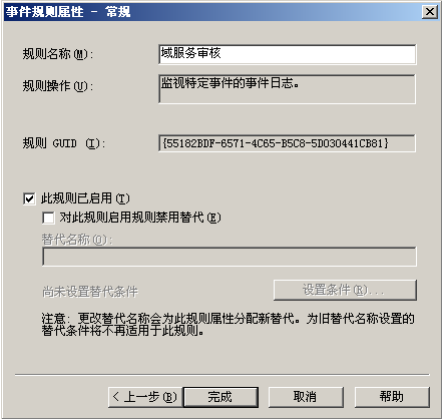


图 18-104 “事件规则属性-常规”对话框

- 11 单击“完成”按钮，创建成功一个新事件规则，如图 18-105 所示。

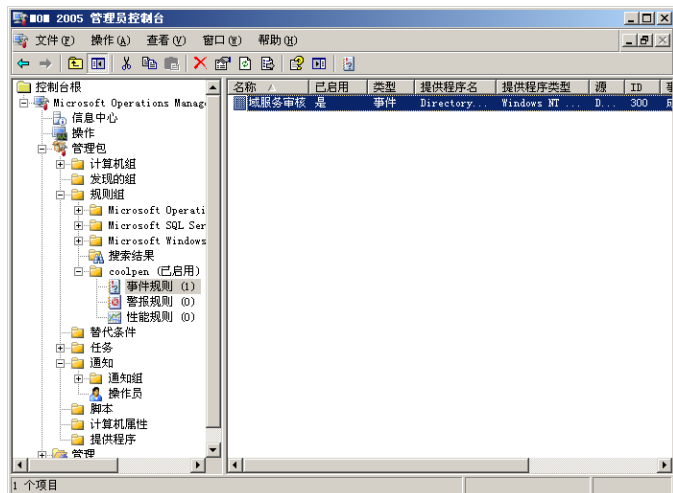


图 18-105 创建成功一个新事件规则

18.6.3 创建警报规则

创建警报规则的操作步骤如下。

① 在“MOM 2005 管理员控制台”窗口中选择“警报规则”选项，右击并选择快捷菜单中的“创建警报规则”选项，显示如图 18-106 所示的“警报规则属性-警报条件”对话框。选中“具有严重性”复选框，并在下拉列表框中选择“服务不可用”选项，同时选中“仅匹配由下列组中的规则生成的警报”复选框。

② 单击“浏览”按钮，显示如图 18-107 所示的“选择规则组”对话框。在规则下拉列表框中选择目标规则，单击“确定”按钮即可。

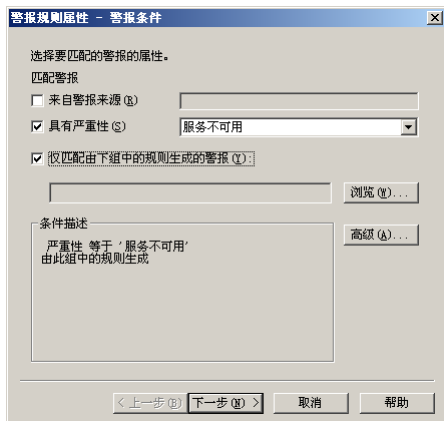


图 18-106 “警报规则属性-警报条件”对话框



图 18-107 “选择规则组”对话框

③ 单击“下一步”按钮，显示如图 18-108 所示的“警报规则属性-计划”对话框，保留默认值即可。

④ 单击“下一步”按钮，显示如图 18-109 所示的“警报规则属性-响应”对话框，在其中根据需要选择响应方式。

⑤ 单击“下一步”按钮，显示如图 18-110 所示的“警报规则属性-知识库”对话框，在其中根据需要设置知识库相关的文档格式及简要说明。

⑥ 单击“下一步”按钮，显示如图 18-111 所示的“警报规则属性-常规”对话框。在“规则名称”文本框中键入规则的名称，选中“此规则已启用”复选框。

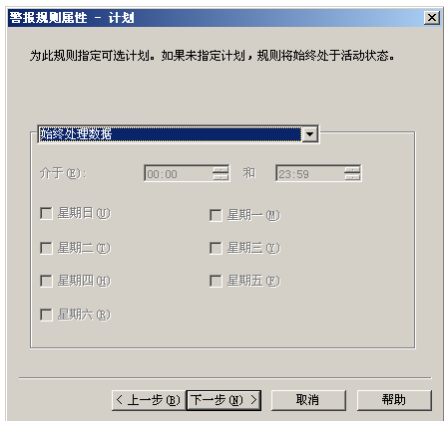


图 18-108 “警报规则属性-计划”对话框

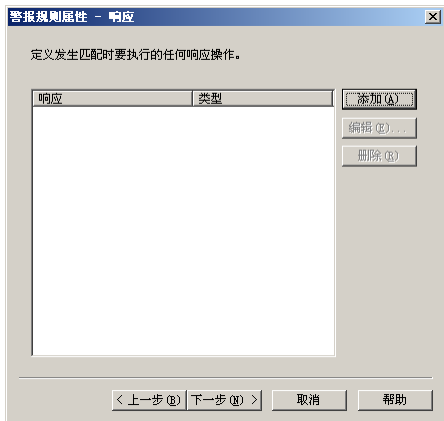


图 18-109 “警报规则属性-响应”对话框



图 18-110 “警报规则属性-知识库”对话框



图 18-111 “警报规则属性-常规”对话框

⑦ 单击“完成”按钮，创建完成新警报规则。

➤➤ 18.6.4 创建性能规则

创建性能规则的操作步骤如下。

- ① 在“MOM 2005 管理员控制台”窗口中选择“性能规则”选项，右击并选择快捷菜单中的“创建性能规则”选项。显示如图 18-112 所示“性能规则类型”对话框，选择“比较性能数据 (阈值)”选项。
- ② 单击“下一步”按钮，显示如图 18-113 所示的“域值规则属性 - 数据提供程序”对话框，在“提供程序名”下拉列表框中选择“DirectoryServices-LDAP Writes/sec-<ALL>-5.0-minutes”程序。

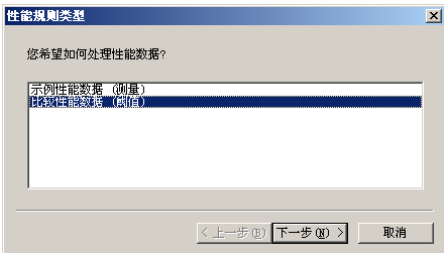


图 18-112 “性能规则类型”对话框

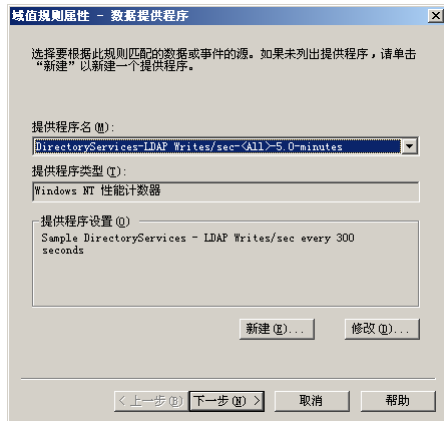


图 18-113 “域值规则属性-数据提供程序”对话框

③ 单击“修改”按钮，显示如图 18-114 所示的“Windows NT 性能计数器提供程序属性”对话框。在其中可以根据需要选择“计数器”和“实例”，单击“确定”按钮关闭。

④ 单击“下一步”按钮，显示如图 18-115 所示的“域值规则属性-计划”对话框，保留默认值即可。

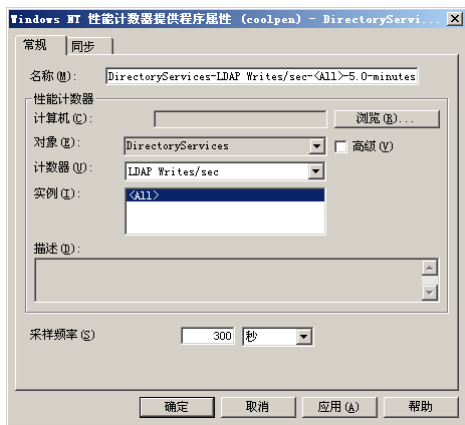


图 18-114 “Windows NT 性能计数器提供程序属性”对话框

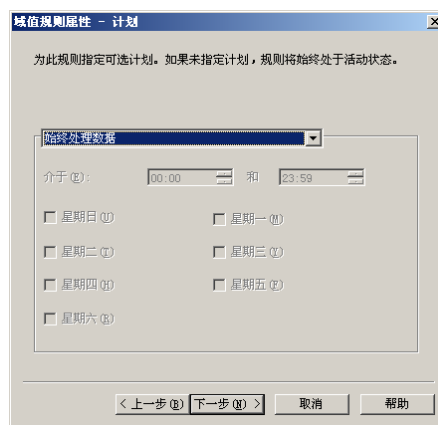


图 18-115 “域值规则属性-计划”对话框

⑤ 单击“下一步”按钮，显示如图 18-116 所示的“域值规则属性-条件”对话框。在其中选中“来自计算机”复选框，在右侧的文本框中键入目标服务器的名称。

⑥ 单击“下一步”按钮，显示如图 18-117 所示的“域值规则属性-阈值”对话框，保留默认值即可。

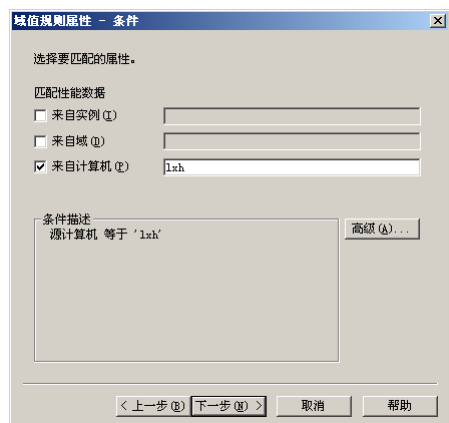


图 18-116 “域值规则属性-条件”对话框

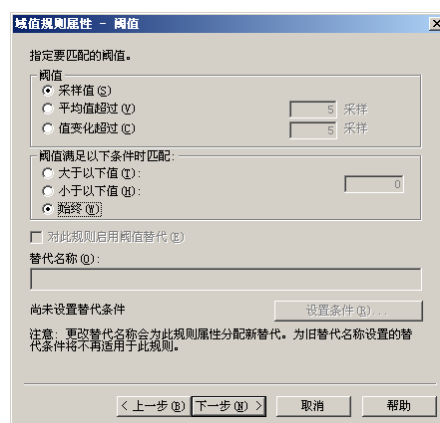


图 18-117 “域值规则属性-阈值”对话框

⑦ 单击“下一步”按钮，显示如图 18-118 所示的“域值规则属性-警报”对话框。选中“生成警报”复选框，在“警报严重性”下拉列表框中选择“错误”选项，在“解决状态”下拉列表框中选择“级别 1：分配给支持人员或本地支持”选项，其他保留默认值即可。

⑧ 单击“下一步”按钮，显示如图 18-119 所示的“域值规则属性-警报抑制”对话框，保留默认值即可。

⑨ 单击“下一步”按钮，显示如图 18-120 所示的“域值规则属性-响应”对话框，在其中可以根据需要设置响应的条件。

⑩ 单击“下一步”按钮，显示如图 18-121 所示的“域值规则属性-知识库”对话框，在其中可以根据需要设置知识库相关的文档格式及简要说明。

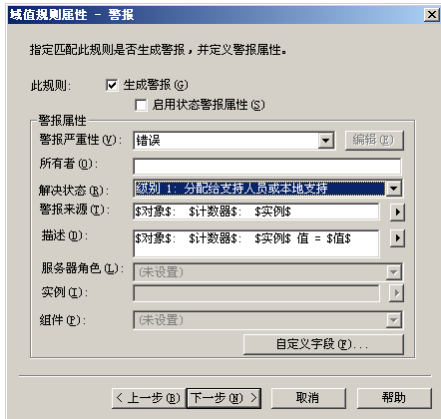


图 18-118 “域值规则属性-警报”对话框

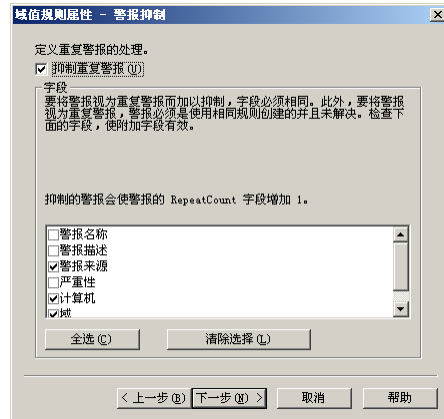


图 18-119 “域值规则属性-警报抑制”对话框



图 18-120 “域值规则属性-响应”对话框



图 18-121 “域值规则属性-知识库”对话框

⑪ 单击“下一步”按钮，显示如图 18-122 所示的“域值规则属性-常规”对话框。在“规则名称”文本框中键入规则的名称，并选中“此规则已启用”复选框。



图 18-122 “域值规则属性-常规”对话框

⑫ 单击“完成”按钮，完成创建新性能规则。

➤➤ 18.6.5 关联规则组和计算机组

在创建规则组时可选择与计算机组关联，但 MOM 2005 内置的一些规则组默认情况下并没有与计算机组关联。如果想使用这些组，应将相应的组与计算机组关联。

(1) 选择规则组，右击并选择快捷菜单中的“与计算机关联”选项，显示如图 18-123 所示的“规

则组属性”对话框。打开“计算机组”选项卡，其中还没有关联任何计算机组。

(2) 单击“添加”按钮，显示如图 18-124 所示的“选择项目”对话框，在其中选择要与该规则组相关联的计算机组。

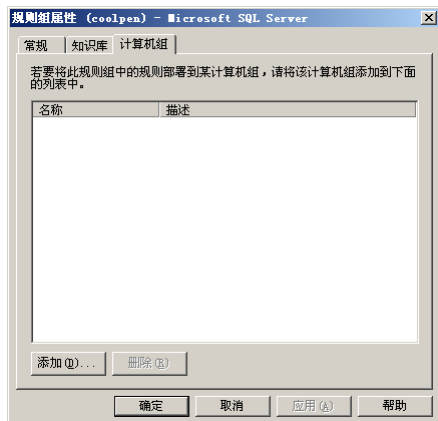


图 18-123 “计算机组”选项卡

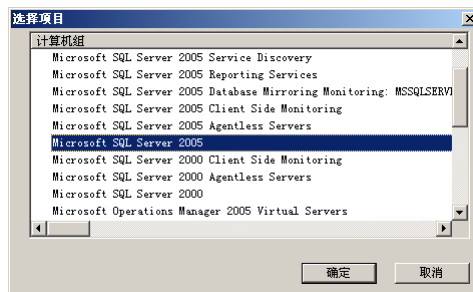


图 18-124 “选择项目”对话框

(3) 依次单击“确定”按钮保存，即可将规则组与计算机组相关联。

18.7 任务

任务是网络管理员在操作员控制台管理目标服务器的方法，在 MOM 2005 中已经内置部分任务。例如，远程桌面、Ping、IP 配置及计算机管理等。管理员可根据需要自定义任务，在导入管理包后也会导入部分管理任务。

18.7.1 创建任务

创建任务的操作步骤如下。

① 在“MOM 2005 管理员控制台”窗口中选择“管理包”→“任务”选项，显示“任务”窗口，如图 18-125 所示。

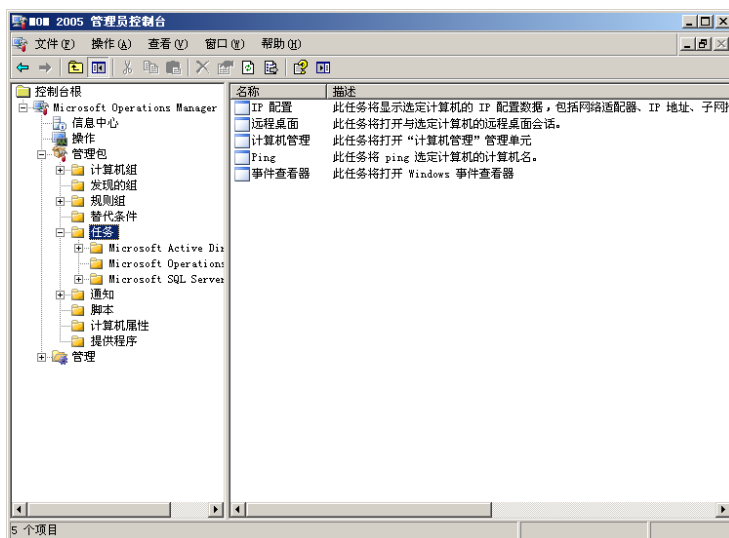


图 18-125 “任务”窗口

② 右击“任务”并选择快捷菜单中的“创建任务”选项，显示如图 18-126 所示的“欢迎使用创建任务向导”对话框。

③ 单击“下一步”按钮，显示如图 18-127 所示的“任务运行位置和类型”对话框。在“运行位置”选项组中选择“代理管理的计算机”单选按钮，在“任务类型”选项组中选择“命令行”单选按钮。

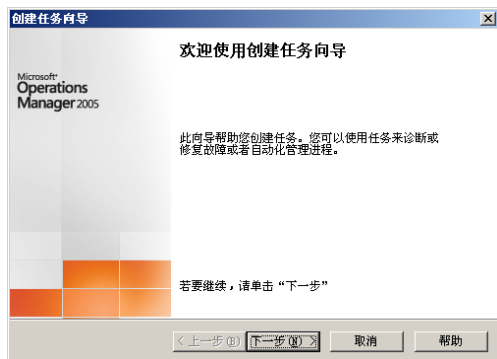


图 18-126 “欢迎使用创建任务向导”对话框

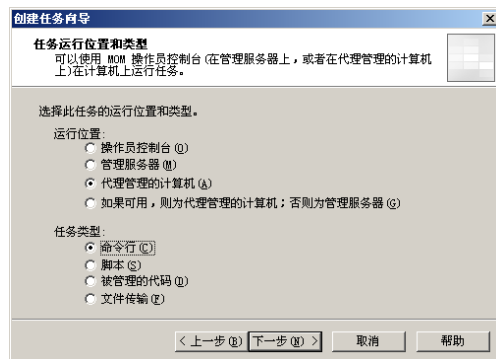


图 18-127 “任务运行位置和类型”对话框

④ 单击“下一步”按钮，显示如图 18-128 所示的“任务配置”对话框，选择“使用 Windows 命令解析器（不推荐）”单选按钮。

⑤ 单击“下一步”按钮，显示如图 18-129 所示的“任务配置”对话框。在“目标角色”下拉列表框中选择“Computer”选项，在“任务命令行”文本框中键入需要执行的命令。这里键入“defrag /a c: >c:\disk.txt”，表示分析 C 盘的磁盘碎片情况，并输入到 disk.txt 文件中。在“任务远程启动目录”下拉列表框中选择命令所在的目标位置，在“任务输出行为”下拉列表框中选择“捕获标准输出。运行任务最长 5 分钟。”选项。



图 18-128 “任务配置”对话框

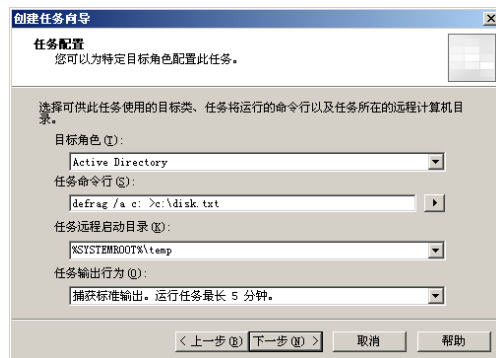


图 18-129 “任务配置”对话框

⑥ 单击“下一步”按钮，显示如图 18-130 所示的“任务名称和描述”对话框。在“名称”文本框中键入任务的名称，在“快捷键”下拉列表框中定义一个快捷键，在“描述”文本框中键入该任务的描述信息。

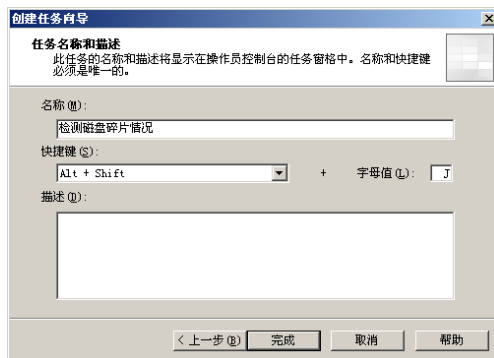


图 18-130 “任务名称和描述”对话框

- ⑦ 单击“完成”按钮，新任务创建完成。
- ⑧ 右击“管理包”选项，在快捷菜单中选择“提交配置更改”选项，将配置更改传输到管理服务器。

18.7.2 编辑任务

MOM 2005 自带了一些任务，网络管理员也可以根据网络的实际情况来修改这些任务。

(1) 在“任务”窗口选择要配置的任务，例如“IP 配置”。右击并选择快捷菜单中的“属性”选项，显示“IP 配置 属性”对话框，在如图 18-131 所示的“常规”选项卡中可以修改“名称”和“快捷键”。

(2) 打开如图 18-132 所示的“详细信息”选项卡，修改该任务的目标角色、应用程序等信息，设置完成后单击“确定”按钮保存设置。

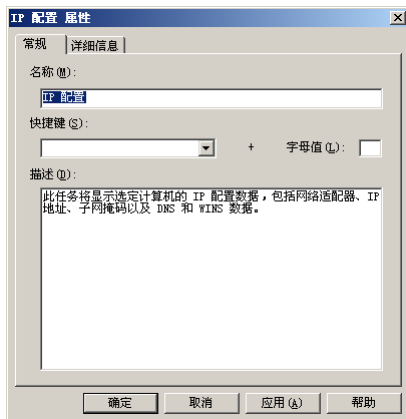


图 18-131 “常规”选项卡

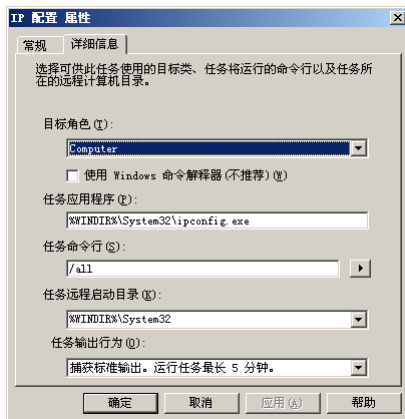


图 18-132 “详细信息”选项卡

18.8 通知

通知设置通知组，当 MOM 2005 监控到预定义的事件或者警报后根据响应设置可以将产生的消息通过电子邮件、短信或消息等方式在第一时间发送给网络管理员，从而提高网络故障的响应时间。

18.8.1 创建通知组

创建通知组的操作步骤如下。

- ① 在“MOM 2005 管理员控制台”窗口中选择“通知”选项，显示如图 18-133 所示的“通知”窗口。



图 18-133 “通知”窗口

② 右击“通知组”并选择快捷菜单中的“创建通知组”选项，显示如图 18-134 所示的“通知组属性-通知组”对话框，在“名称”文本框中键入新通知组的名称。

③ 单击“新建操作员”按钮，显示如图 18-135 所示的“操作员属性-常规”对话框，选中“已启用”复选框。

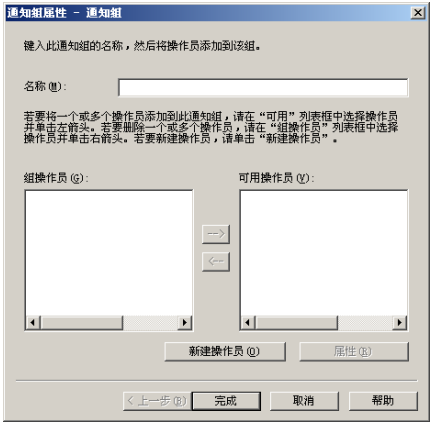


图 18-134 “通知组属性-通知组”对话框



图 18-135 “操作员属性-常规”对话框

④ 单击“下一步”按钮，显示如图 18-136 所示的“操作员属性-电子邮件”对话框。选中“向此操作员发送电子邮件”复选框，在“电子邮件地址”文本框中键入操作员使用的电子邮件地址，选择“始终向此操作员发送电子邮件”单选按钮。

⑤ 单击“下一步”按钮，显示如图 18-137 所示的“操作员属性-页面”对话框，保留默认值即可。

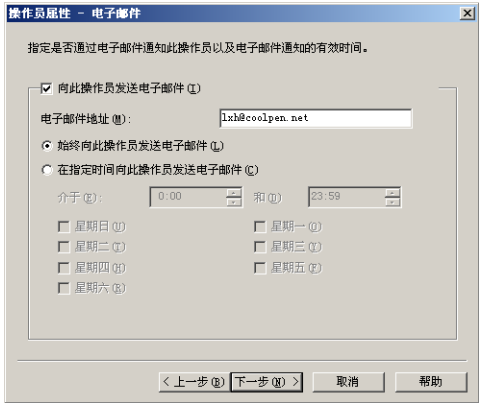


图 18-136 “操作员属性-电子邮件”对话框

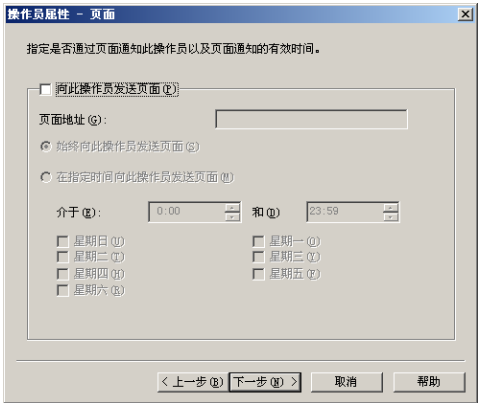


图 18-137 “操作员属性-页面”对话框

⑥ 单击“下一步”按钮，显示如图 18-138 所示的“操作员属性-命令”对话框，保留默认值即可。

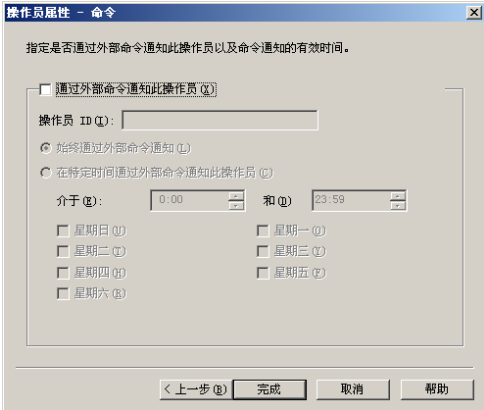


图 18-138 “操作员属性-命令”对话框

⑦ 单击“完成”按钮，关闭操作员属性设置向导，显示如图 18-139 所示的“操作员属性-通知组”对话框，在“可用操作员”列表框中选择操作员。

⑧ 单击“<-”按钮，将操作员添加到“组操作员”列表框中，如图 18-140 所示。

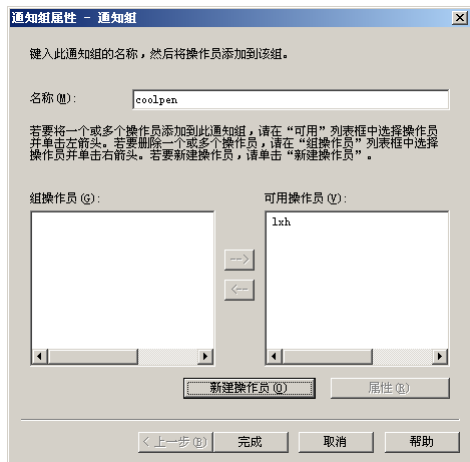


图 18-139 “操作员属性-通知组”对话框

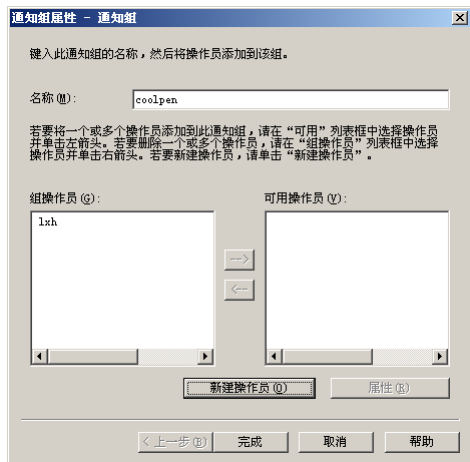


图 18-140 将操作员添加到“组操作员”列表框中

⑨ 单击“完成”按钮，创建完成通知组。

18.8.2 关联操作员到通知组

MOM 2005 默认自带了 4 个通知组，用户可以根据需要在不同的通知组中添加操作员。以“Network Administrators”组为例，右击该组。选择快捷菜单中的“属性”选项，显示如图 18-141 所示的通知组属性对话框，可在该通知组中添加操作员。

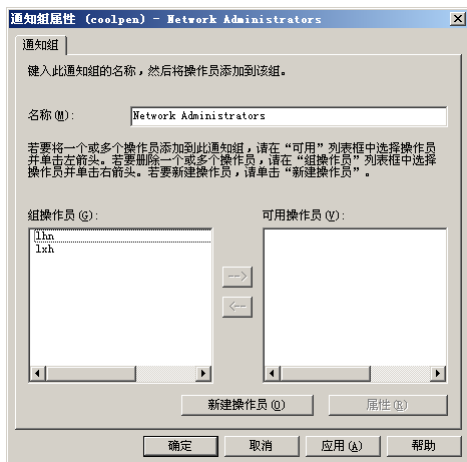


图 18-141 通知组属性对话框

18.9 操作员控制台

操作员控制台是 MOM 2005 监控和处理目标服务器异常的工作平台，可以处理目标服务器产生的事件及警报等异常信息。同时可以监控目标服务器的性能和状态，并可派发维护任务。自动完成目标服务器的监控和管理，提高管理效率。

18.9.1 处理警报

处理警报的操作步骤如下。

① 单击“开始”→“所有程序”→“Microsoft Operations Manager 2005”→“操作员控制台”选项，显示如图 18-142 所示的“Microsoft Operations Manager 2005 操作员控制台”窗口。在工具栏上的“组”列表框中可以选择当前登录的操作员的作用域，默认为当前操作用户顶级根。

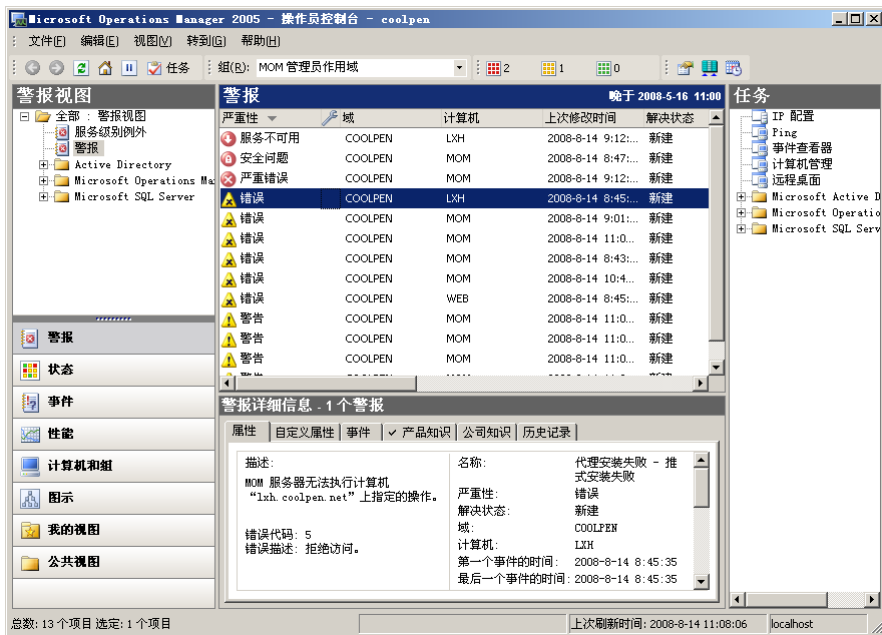


图 18-142 “Microsoft Operations Manager 2005 操作员控制台”窗口

② 在操作员控制台的“警报”区域可以查看警报列表。选择一个警报，在“警报详细信息-1 个事件”区域中显示警报相关信息。默认显示“属性”选项卡，可以看到产生警报的规则、关联的事件，以及问题的严重性等信息。

③ 打开如图 18-143 所示的“事件”选项卡，显示该警报关联的事件。

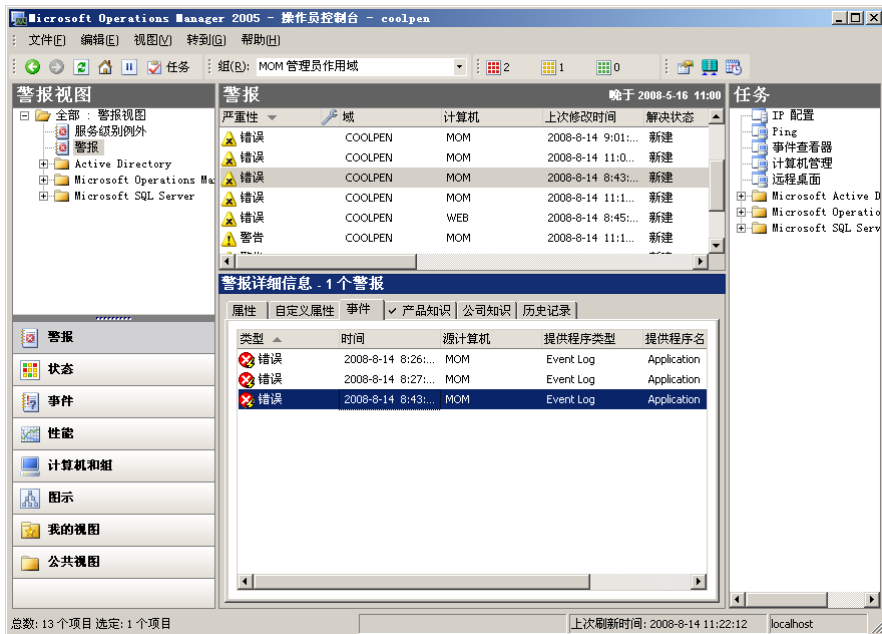


图 18-143 “事件”选项卡

④ 打开如图 18-144 所示的“产品知识”选项卡，其中显示该规则关联的由微软公司提供的知识库。

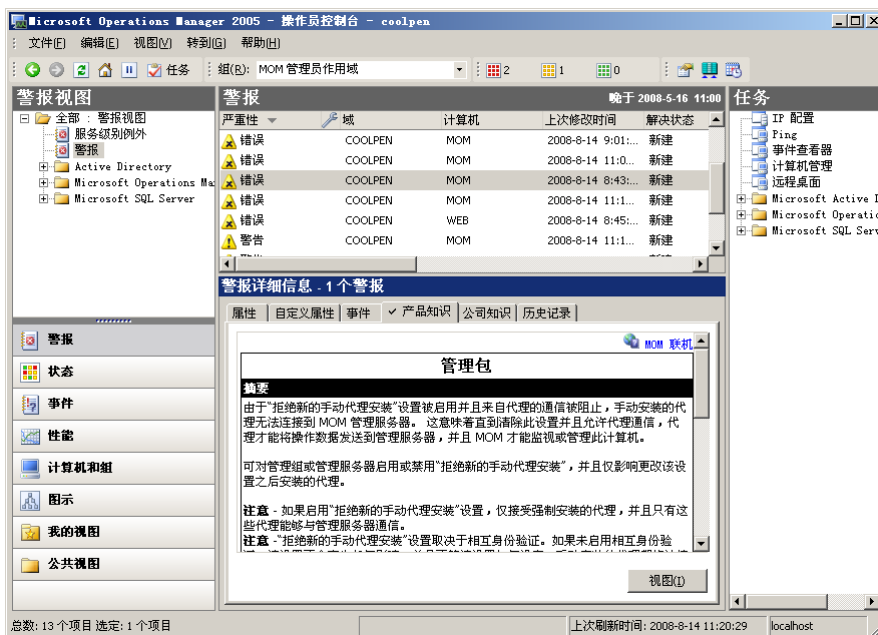


图 18-144 “产品知识”选项卡

- ⑤ 单击“视图”按钮，显示知识库的详细信息，如图 18-145 所示。

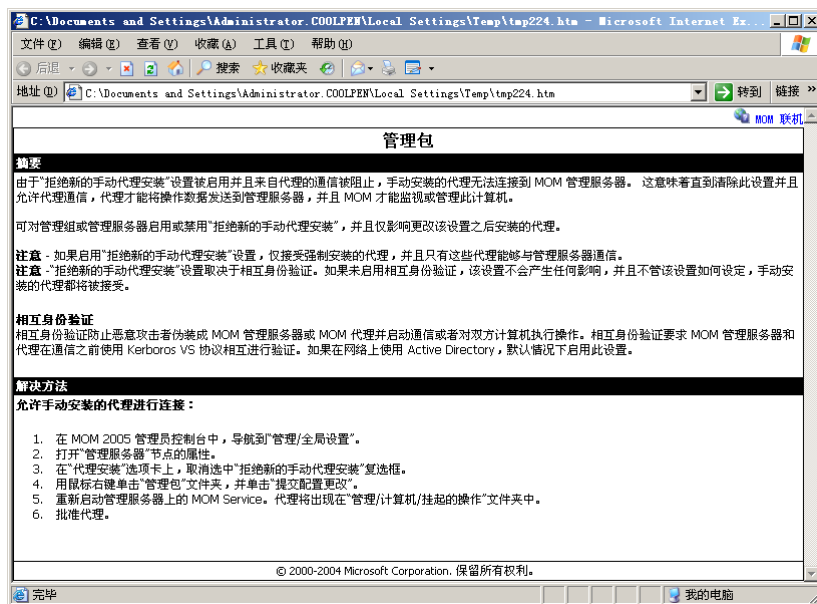


图 18-145 知识库的详细信息

⑥ 打开“公司知识”选项卡，如图 18-146 所示。单击“编辑”按钮，可以编辑处理该事件或者警报的维护记录或联系人信息。在出现类似的警报时，可以查看网络管理员曾经处理此类问题的解决方法，加快排除故障的速度并提高工作效率。

⑦ 打开“历史记录”选项卡，如图 18-147 所示。其中显示该警报的历史记录信息。单击“附加”按钮，可以设置该警报关联的信息。

如果某个警报相关的事件已经解决，即可将其设置为“已解决”，已解决的警报将不再显示在警报窗口中。选择警报，右击在快捷菜单中选择“设置警报解决状态”→“已解决”选项，显示如图 18-148 所示的“解决警报”对话框。键入解决该警报的方法及问题描述信息，单击“确定”按钮即可。

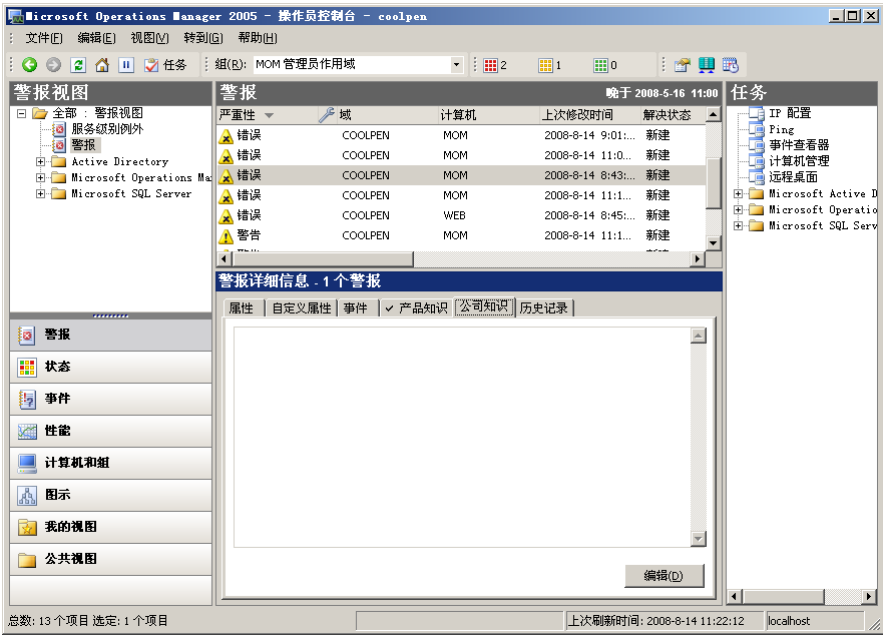


图 18-146 “公司知识”选项卡

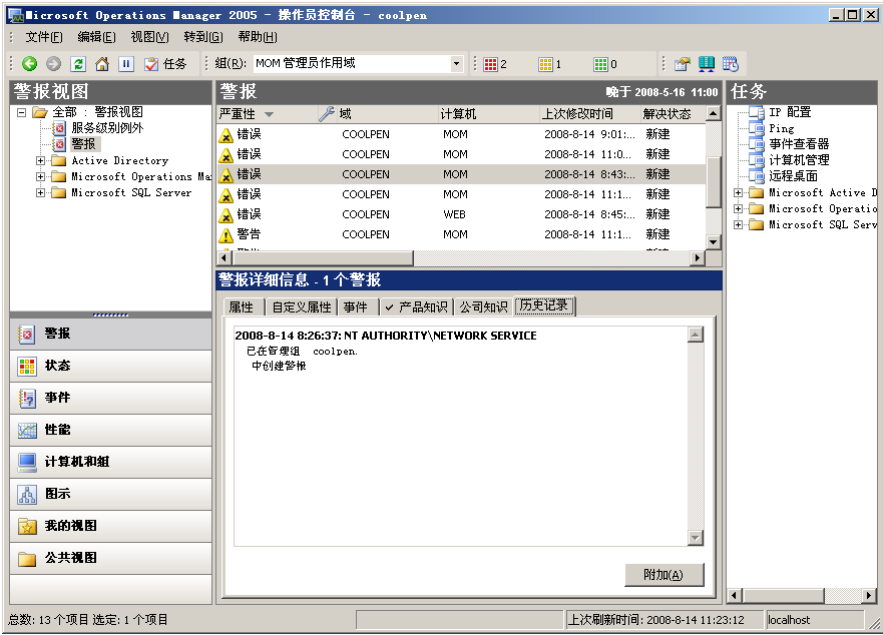


图 18-147 “历史记录”选项卡

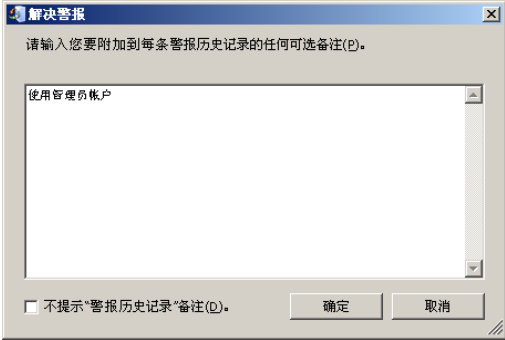


图 18-148 “解决警报”对话框

18.9.2 图示

在操作员控制台窗口中选择视图区域的“图示”选项，显示当前视图的关联视图，如图 18-149 所示。

单击工具栏中的“查看图示示例”按钮，显示如图 18-150 所示“图例”对话框。其中列出不同图标所代表的意义，从而可以查看当前监控的服务器状态。

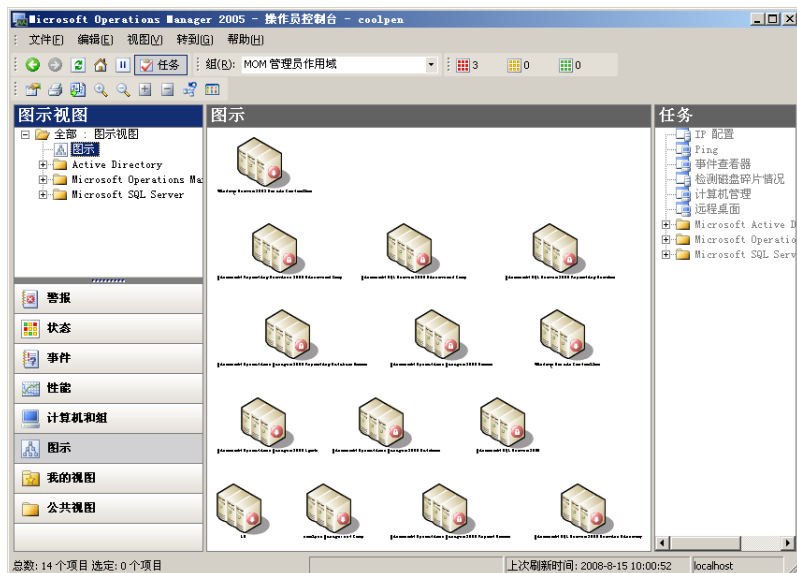


图 18-149 当前视图的关联视图



图 18-150 “图例”对话框

18.9.3 事件

事件视图包括事件和任务状态两大类，用其可以查看各个任务的执行状态及结果等详细信息。

在操作员控制台中选择“事件”选项，在“事件视图”列表框中默认选择一个事件，在“详细信息”区域中显示该事件的详细信息，如图 18-151 所示。

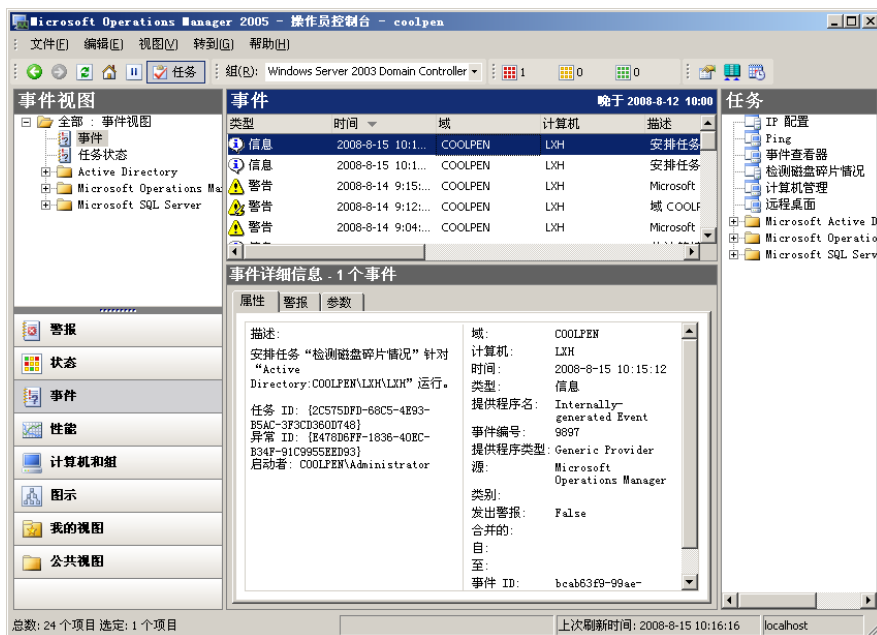


图 18-151 事件的详细信息

在“事件视图”列表框中选择“任务状态”选项，选择一个任务。在“详细信息”区域显示该任务的执行状态及结果，如图 18-152 所示。

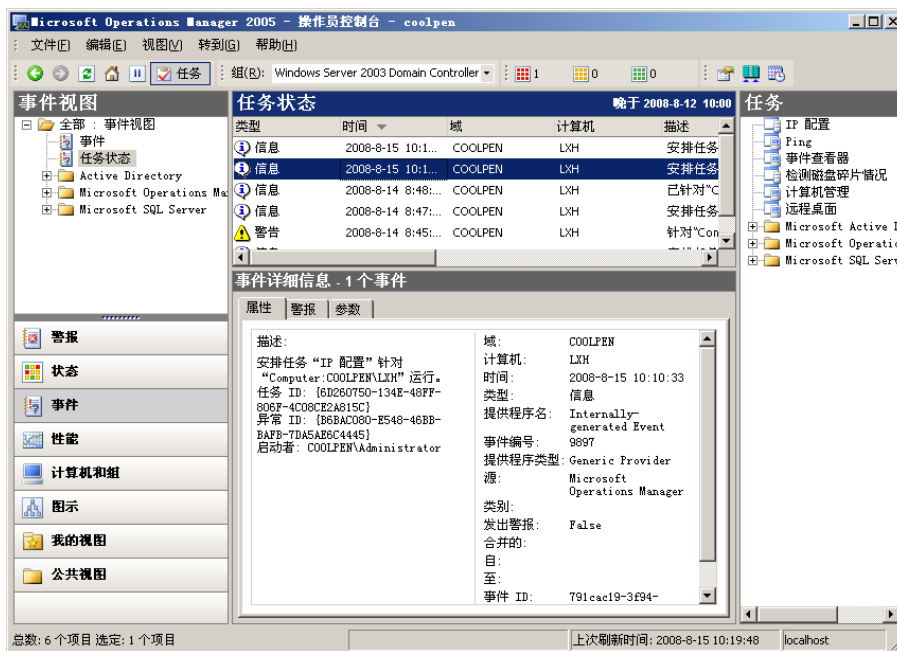


图 18-152 任务的执行状态及结果

18.9.4 状态

在状态视图中可以查看所有的警报信息，包括目标服务器警报的状态及发生的事件等。

在操作员控制台中选择“状态”视图，在“状态”列表框中显示警报的状态，如图 18-153 所示。

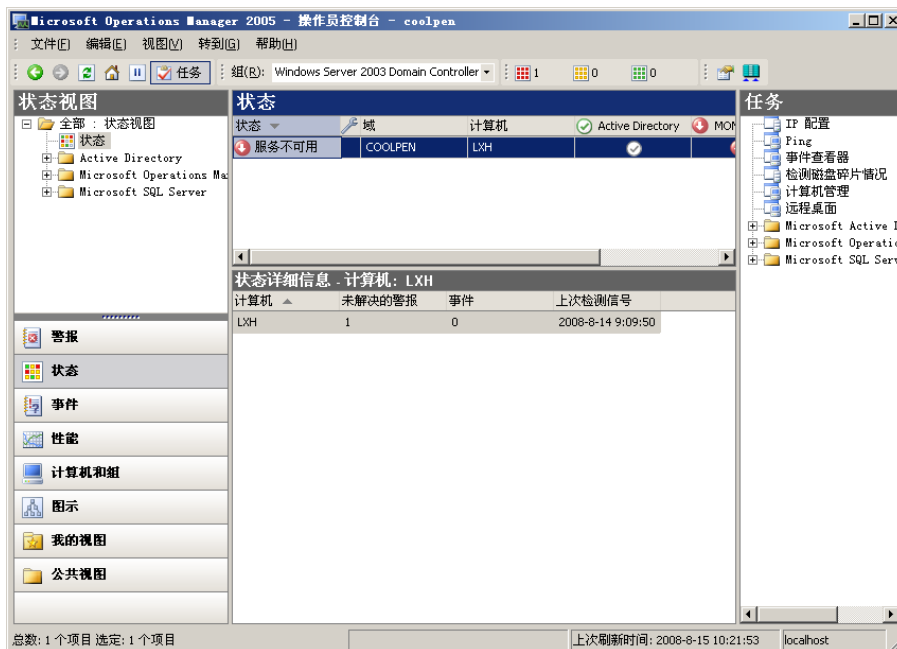


图 18-153 警报的状态

选择一个警报，右击并从快捷菜单中选择“视图”→“事件”选项。显示目标服务器产生的所有事件，如图 18-154 所示。



图 18-154 所有事件

18.9.5 性能

在操作员控制台中选择“性能”视图，显示操作员具备权限访问的目标服务器列表，如图 18-155 所示。

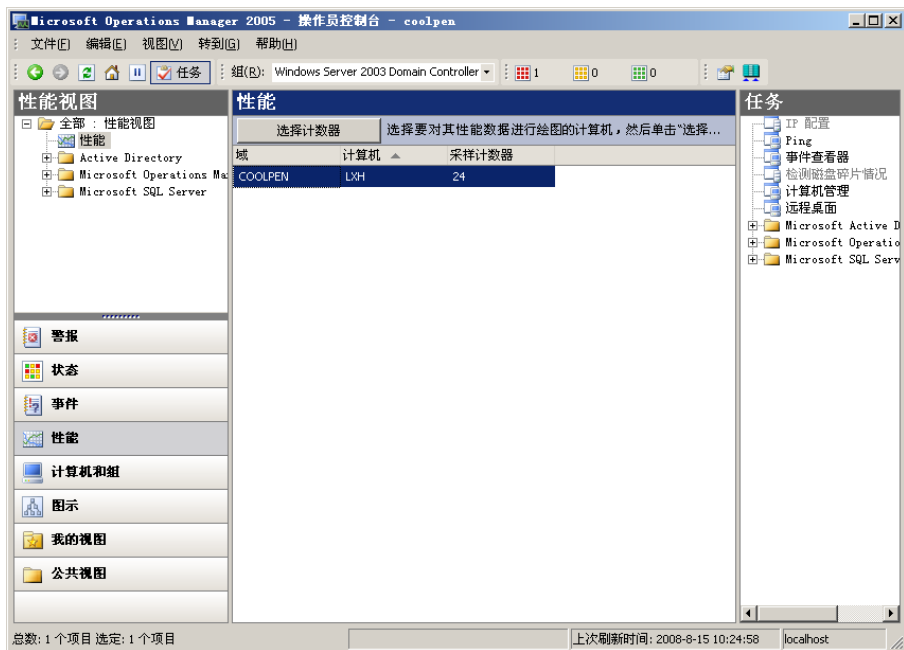


图 18-155 操作员具备权限访问的目标服务器列表

选择目标服务器，单击“选择计数器”按钮，显示如图 18-156 所示的选定计算机的“性能计数器”窗口。

选择目标计数器，单击“绘制图形”按钮。显示如图 18-157 所示的“性能图”窗口，其中以图形方式显示性能计数的情况。

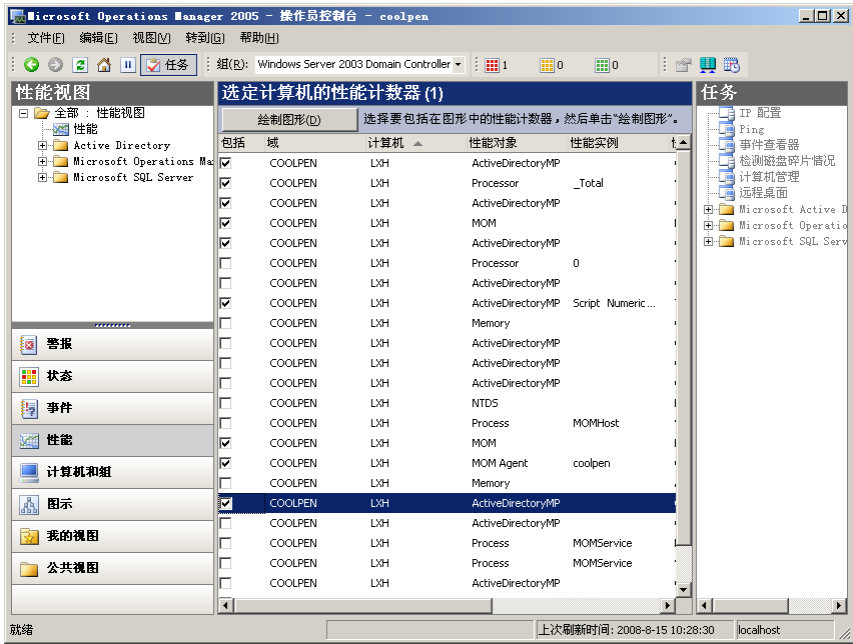


图 18-156 “性能计数器”窗口

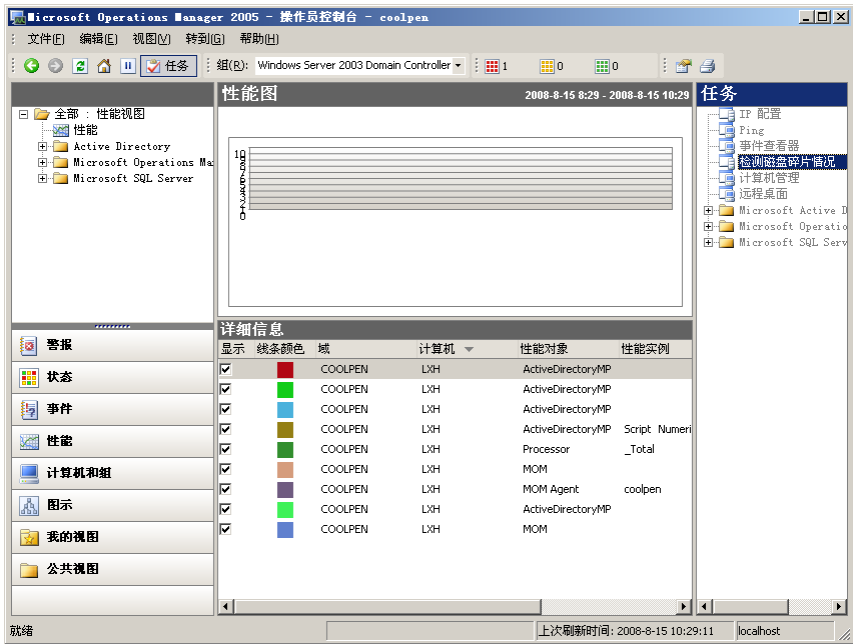


图 18-157 “性能图”窗口

➤➤ 18.9.6 计算机和组

在操作员控制台中，选择如图 18-158 所示的“计算机和组”视图，在“计算机”窗口中可以查看目标服务器列表。选择目标服务器，在“计算机详细信息”区域中的“属性”选项卡中显示当前计算机中可以监控的 MOM 管理包。

打开如图 18-159 所示的“规则组”选项卡，显示规则组关联的计算机组和计算机组关联的计算机列表。

打开如图 18-160 所示的“计算机组”选项卡，显示目标服务器所关联的计算机组，以及描述信息。

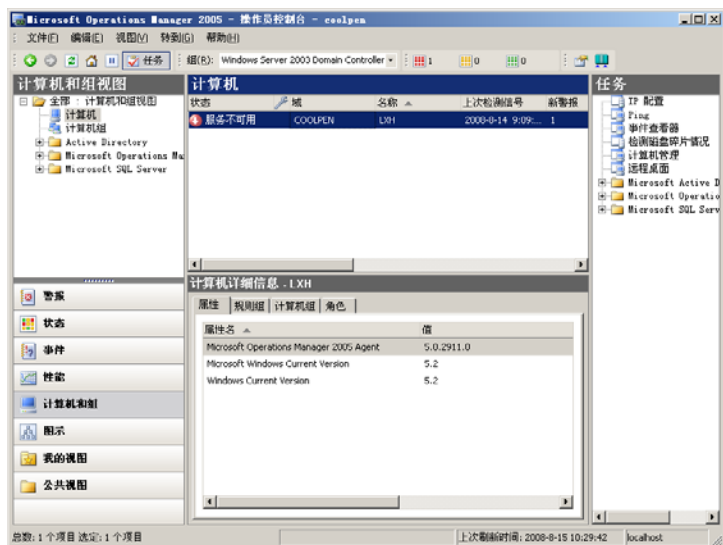


图 18-158 “计算机和组”视图

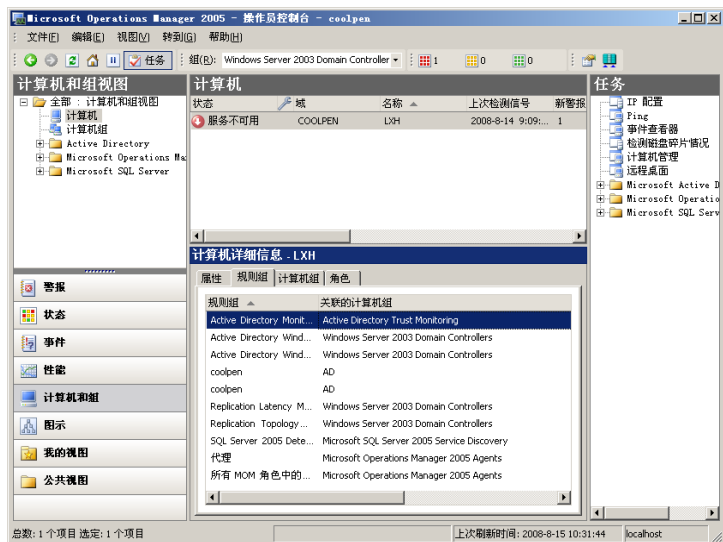


图 18-159 “规则组”选项卡

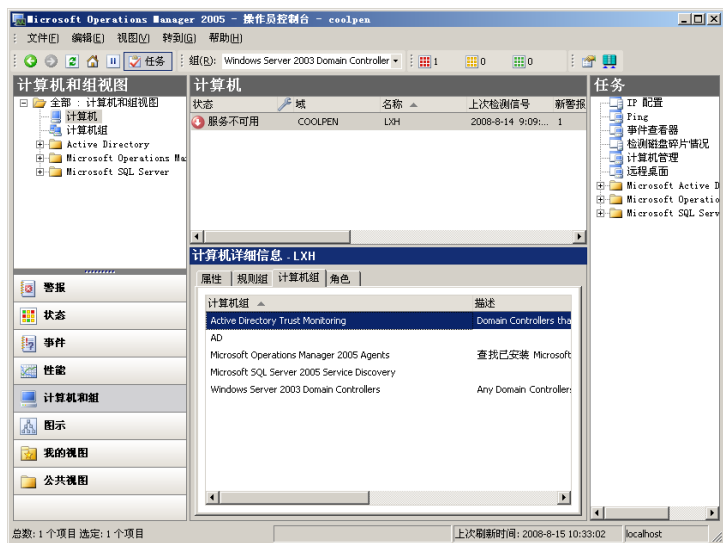


图 18-160 “计算机组”选项卡

打开如图 18-161 所示的“角色”选项卡，其中显示选择的服务器中关联的 MOM 2005 规则组件列表。

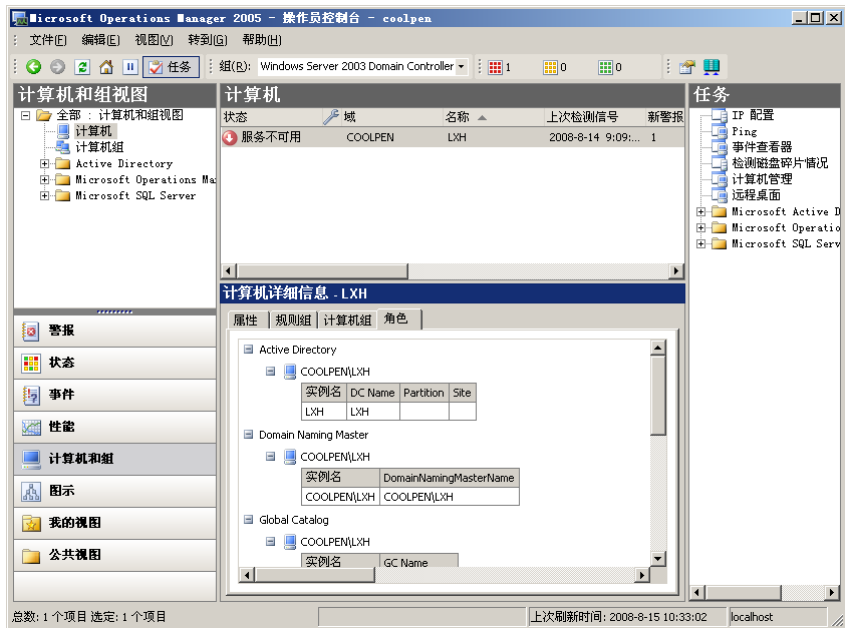


图 18-161 “角色”选项卡

18.9.7 任务

在“操作员控制台”窗口右侧的“任务”区域中显示 MOM 中配置的所有任务，网络管理员在其中可以运行已有的任务。

① 以前面所配置的“检测磁盘碎片情况”任务为例，右击“检测磁盘碎片情况”任务。从快捷菜单中选择“运行任务”选项，显示如图 18-162 所示的“欢迎使用任务向导”对话框。

② 单击“下一步”按钮，显示如图 18-163 所示的“命令行任务参数”对话框，默认显示曾经配置的命令行参数。

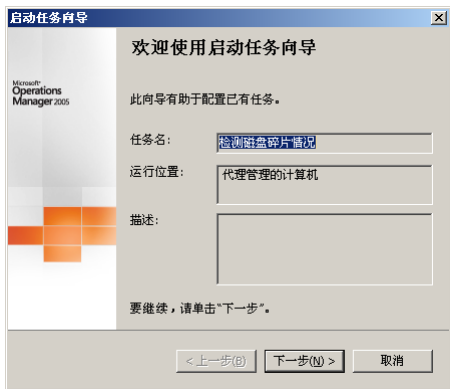


图 18-162 “欢迎使用任务向导”对话框

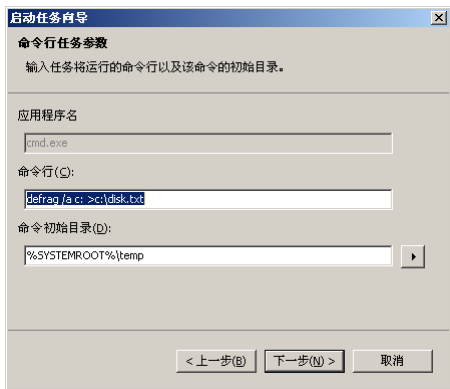


图 18-163 “命令行任务参数”对话框

③ 单击“下一步”按钮，显示如图 18-164 所示的“任务目标”对话框，在“目标”列表框中选择目标服务器。

④ 单击“下一步”按钮，显示如图 18-165 所示的“完成启动任务向导”对话框。

⑤ 单击“完成”按钮，关闭任务向导。



图 18-164 “任务目标”对话框

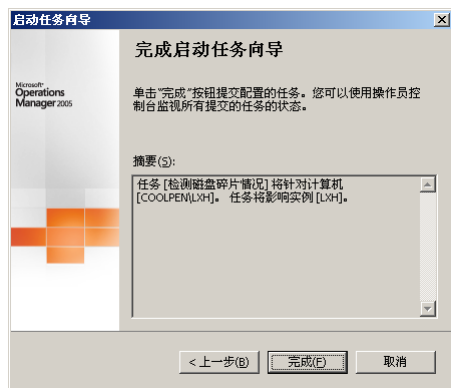


图 18-165 “完成启动任务向导”对话框

第 19 章 配置与管理 ISA 服务

防火墙是网络必不可少安全防护功能, ISA Server 2006 是 Microsoft 推出的一款优秀的防火墙软件, 并且具有代理服务器功能。不仅可以将网络中的各种服务发布到 Internet, 提供安全的 VPN 连接功能, 还可以为客户端提供 Internet 连接共享。同时, ISA Server 的代理服务器提供了“Web 缓存”功能, 可作为企业的缓存服务器为网络用户提供较快的 Web 访问速度。

19.1 ISA Server 2006 概述

ISA Server 2006 同时具有防火墙、代理服务器和缓存 3 大功能, 不仅能够实现 Internet 连接共享。还可以通过制定策略及规则控制网络内部与外部的通信, 防范外来网络的攻击。从而提高网络性能和安全性, 使客户端最大限度利用现有网络投资。

►► 19.1.1 ISA Server 2006 功能简介

1. 代理服务器功能

只要将网络 and 用户连接到 Internet, 就难免会有安全性和效率问题。ISA Server 2006 可以控制每个用户的访问并监视使用率, 保护网络免受未经授权的访问、执行状态筛选和检查, 并在防火墙或受保护的网路受到攻击时向网络管理员发出警报。

ISA Server 作为防火墙, 通过数据包级别、电路级别和应用程序级别的通信筛选、状态筛选和检查、广泛的网路应用程序支持、紧密地集成虚拟专用网路 (VPN)、系统坚固、集成的入侵检测、智能的第 7 层应用程序筛选器、对所有客户端的防火墙透明性、高级身份验证, 以及安全的服务器发布等增强安全性实现的功能如下。

- (1) 保护网路免受未经授权的访问。
- (2) 保护 Web 和电子邮件服务器防御外来攻击。
- (3) 检查传入和传出的网路通信以确保安全性。
- (4) 接收可疑活动警报。

2. 加快 Web 访问速度

在网路中每个 Internet 的用户都会占用一定带宽, 当同时访问用户过多时就会造成 Internet 链路阻塞。ISA Server 2006 可以提供本地缓存, 将 Web 内容的性能瓶颈控制在最少并节省网路带宽。ISA Server 2006 可实现如下功能。

- (1) 通过从 Web 缓存 (而非 Internet) 提供对象来提高用户的 Web 访问速度。
- (2) 通过减少链路上的网路通信来减少 Internet 带宽成本。
- (3) 分布 Web 服务器内容和电子商务应用程序, 从而有效地覆盖全世界的客户并有效地控制了成本。
- (4) 从 ISA Server Web 缓存中提供常用的 Web 内容, 并将节省的内部网路带宽用于其他内容请求。

3. 虚拟专用网路 (VPN) 支持

ISA Server 2006 支持安全的 VPN 访问, 使分支机构或远程用户可以通过 VPN 连接到公司网路。ISA Server 防火墙策略应用于 VPN 连接, 控制 VPN 用户可以访问的资源 and 协议。

4. 安全发布服务器

当来自 Internet 的用户访问部署了防火墙的局域网时就会受到防火墙的阻止, 而 ISA Server 2006 可以将局域网内的多台服务器和多种服务发布到 Internet, 为 Internet 中的用户提供相应的服务。在 ISA Server 2006 中使用一个或多个公网地址即可同时发布受 ISA Server 保护的网内的所有服务器和服务, 真正地发布安全的 Web 站点, 这些都是其他软件或硬件防火墙所不能比拟的。

19.1.2 ISA Server 2006 中的网络

在 ISA Server 2006 的网络中, 分为“内部”、“外部”、“本地主机”、“VPN 客户端”和“被隔离的 VPN 客户端”共 5 个部分。这些网络的功能和意义分别如下。

(1) 内部: 代表内部局域网, ISA 防火墙将内部网络代表受信任的受保护的网, 其默认防火墙策略允许本地主机访问内部网络上的资源。但拒绝其他任何网络访问内部网络, 用户必须创建规则来允许访问内部网络。

(2) 本地主机: 代表 ISA Server 本身计算机, 与 ISA 防火墙之间的所有通信都被认为是和本地主机网络之间的通信。

(3) 外部: 指连接到 Internet 的网络, 通常被视为不受信任的网络。

(4) VPN 客户端: 代表通过 VPN 连接到 ISA 服务器的客户端, 由 ISA 防火墙动态生成。

(5) 被隔离的 VPN 客户端: 包含尚未解除隔离的 VPN 客户端的地址, 由 ISA 防火墙动态生成。

除了上述 5 个部分网络, 如果 ISA Server 被配置成“3 向外围网络”, 还包括“外围”网络。“外围”网络也称为“DMZ”(Demilitarized Zone), DMZ 通常用于放置公共信息, 用户、潜在用户和外部访问者都可以直接访问 DMZ 区域, 而不必通过内网。目前, 许多硬件防火墙都集成了 DMZ 接口。ISA Server 2006 也可以在安装 3 块网卡(或者更多)的情况下, 配置成“3 向外围网络”。

19.1.3 ISA Server 2006 的客户端

ISA Server 2006 包括 3 种类型的客户端, 分别为“防火墙客户端”、“SecureNAT 客户端”和“Web 代理客户端”, 其意义如下。

(1) 防火墙客户端: 已经安装并启用防火墙客户端软件的计算机, 来自防火墙客户端的请求会定向到 ISA Server 计算机上的防火墙服务, 以确定是否允许访问, 此后可以使用应用程序筛选器和其他插件对这些请求进行筛选。防火墙服务还可以缓存所请求的对象, 或者从 ISA Server 缓存提供对象。

(2) SecureNAT 客户端: 指尚未安装防火墙客户端软件的计算机。来自 SecureNAT 客户端的请求首先会定向到网络地址转换(NAT)驱动程序, 使用 Internet 中有效的全局 IP 地址替换 SecureNAT 客户端的内部 IP 地址。然后该客户端请求会定向到防火墙服务, 以确定是否允许访问。最后可以使用应用程序筛选器和其他扩展组件对该请求进行筛选。防火墙服务还可以缓存所请求的对象, 或者从 ISA Server 缓存提供对象。通常情况下, 大多数的客户端和将要使用 ISA Server 发布的服务器都必须是“SecureNAT 客户端”。

(3) Web 代理客户端: 指与 CERN 兼容的 Web 应用程序。来自 Web 代理客户端的请求会定向到 ISA Server 计算机上的防火墙服务, 以确定是否允许访问。防火墙服务还可以缓存所请求的对象, 或者从 ISA 服务器缓存提供对象。“防火墙客户端”和“SecureNAT”客户端必须是 ISA Server “内网”中的计算机, 而“Web 代理客户端”可以是 Internet 上的计算机。

无论客户端的类型如何, 当 ISA Server 接收到 HTTP 请求时客户端都被视为 Web 代理客户端, 这对于验证该客户端身份的方式具有特定的含义。

防火墙客户端和 SecureNAT 客户端都可以作为 Web 代理客户端。如果将计算机上的 Web 应用程序明确配置为使用 ISA Server, 则所有 Web 请求将直接发送到防火墙服务, 包括 HTTP、FTP 和安全 HTTP (HTTPS); 否则防火墙服务将首先处理所有其他请求。

19.2 应用 ISA Server

ISA Server 2006 可以应用到各种规模的网络中，在 Internet 边缘、部门或主干网络及分支办公室等位置均可提供不同的功能与服务，并且可以将网络内部的服务器发布到 Internet。ISA Server 2006 提供了不同的模板，以用于不同的网络。

19.2.1 Internet 边缘防火墙

ISA Server 可以部署为专用 Internet 边缘防火墙来充当内部客户端的 Internet 安全网关。ISA Server 计算机对于通信路径上的其他方来说是透明的，Internet 用户无法判断此处是否有防火墙服务器；除非用户试图访问 ISA Server 计算机拒绝访问的网络服务、协议或站点。通过设置安全访问策略，网络管理员可以防止未经授权的访问和恶意内容进入网络。这些功能如下。

- (1) 多层通信筛选包括数据包级别、线路级别和应用程序级别筛选。
- (2) 智能应用程序层警示应用程序筛选器。
- (3) 内置入侵检测。
- (4) 锁定基本操作系统的系统强化。

19.2.2 部门或主干网络防火墙

ISA Server 可以配置为部门或主干网络防火墙，为进出受保护的局域网提供安全的入站和出站访问控制。用户通常希望将高性能防火墙部署在 Internet 边缘，而将复杂应用程序层筛选分配到位于局域网边缘的 ISA Server 防火墙。这样用户既可以充分利用 ISA Server 应用程序层筛选防火墙提供的独特级别保护，又可充分利用现有的高速 Internet 连接。这些功能如下。

- (1) 安全 OutlookWebAccess 发布。
- (2) 安全 Internet 信息服务 (IIS) 网站发布。
- (3) 安全 Exchange RPC 发布。
- (4) 所有 Internet 协议和服务基于用户和基于组的访问控制。
- (5) 垃圾邮件筛选的 SMTP 消息筛选程序。
- (6) 与上游 Web 代理服务器链接的 Web 代理。

19.2.3 分支办公室防火墙

通过 ISA Server 可以使用站点到站点的 VPN 连接，将分支办公室网络连接到主网络。可以将 ISA Server 放置在分支办公室，作为保护分支办公室网络的防火墙，也可以将分支办公室网络连接到主办公室网络的 VPN 网关。ISA Server 具有经过改进的 VPN 互操作性功能，用户可以使用当前拥有的任何 VPN 解决方案创建站点到站点的链接。这些功能如下。

- (1) Internet 协议安全 (IPSec) 隧道模式支持使用第三方 VPN 网关的站点到站点链接。
- (2) 使用 Microsoft VPN 网关的站点到站点链接的点对点隧道协议 (PPTP) 和 IPSec 上的第 2 层隧道协议 (L2TP)。
- (3) 对站点到站点链接的监控状态检测限制可以访问主办公室网络的远程网络。
- (4) 位于分支办公室的用于与 Internet 之间的入站和出站访问的 ISA Server 防火墙控制。
- (5) 检测 VPN 连接的 LAN 之间的通信监控状态的智能应用程序层筛选。

19.2.4 发布安全服务器

ISA Server 允许企业可以在不危及内部网络安全的情况下将服务发布到 Internet，组织可以配置

Web 发布规则和服务器发布规则来确定哪些请求向下游发送到位于 ISA 服务器防火墙后的服务器，以便为内部服务器提供增强的安全层。所有转发的通信对 ISA 服务器的监控状态筛选和检测引擎都是公开的。例如，Microsoft Exchange 服务器放置在 ISA 服务器后，可以创建服务器发布规则来允许对 Exchange 简单邮件传输协议（SMTP）、POP3、Internet 邮件访问协议（IMAP4）和网络对网络传输协议（NNTP）服务进行 SSL 保护的远程访问。ISA Server SMTP 消息筛选程序对传入到 Exchange 服务器的电子邮件进行侦听，然后其消息筛选程序可以对 SMTP 通信进行筛选，并将其转发给 Exchange 服务器。Exchange 服务器从不直接对外部用户公开。而是保留在安全的环境中，维护对其他内部网络服务的访问。这些功能如下。

- (1) 易于使用的安全服务器发布向导。
- (2) 用于透明客户端连接和服务器发布的 SecureNAT。
- (3) 已发布的服务，包括超文本传输协议/安全套接字层（HTTP/SSL）、FTP、SMTP、POP3、IMAP4、NNTP、DNS、RDP、H.323 及流媒体等。

19.3 部署 ISA Server 2006

ISA Server 2006 分为标准版和企业版，二者的基本功能相同，如安装连接 Internet（作代理服务器）、发布服务器及缓存等。但标准版不支持“阵列”功能，而企业版可以利用多台服务器组成 ISA 阵列。ISA Server 2006 对服务器的软件与硬件配置都有一定的要求，而且所连接的客户端越多，所要求的配置也越高。

19.3.1 安装 ISA Server 2006 的软件与硬件需求

要安装使用 ISA 服务器，需要满足以下条件。

- (1) 具有 550 MHz 或更高频率的兼容 Pentium II 的 CPU 的个人计算机。
- (2) 服务器采用 Windows Server 2003 操作系统。
- (3) 至少 256 MB 内存（推荐 1 GB 以上）。
- (4) 至少两块网络适配器，一块用于与内部网络通信；另一块用于连接外部网络。
- (5) 磁盘分区采用 NTFS 文件系统，并且至少拥有 150 MB 的可用空间用于缓存及至少 4 GB 的可用空间用于记录 Microsoft SQL Serve 2000 Desktop Engine（MSDE 2000）或文本文件。

每台 ISA Server 2006 服务器大约（最大同时）能连接 500 个~1 000 个客户端，如果企业中的计算机超过这个数量，或者虽然没有超过这个数量，但想实现高性能及高安全性（在发生服务器硬件故障时不中断服务），需要使用 ISA Server 2006 企业版组成“阵列”方式。

19.3.2 安装 ISA Server 2006

安装 ISA Server 2006 的操作步骤如下。

- ① 将 ISA Server 2006 安装光盘放入光驱，光盘自动运行，显示如图 19-1 所示的“Microsoft ISA Server 2006 安装程序”窗口。
- ② 单击“安装 ISA Server 2006”选项，启动 Microsoft ISA Server 2006 安装向导，如图 19-2 所示。
- ③ 单击“下一步”按钮，选择“我接受许可协议中的条款”单选按钮，许可对话框如图 9-13 所示。
- ④ 单击“下一步”按钮，显示如图 19-4 所示的“客户信息”对话框。分别在“用户名”和“单位”文本框中键入用户名称和单位信息，在“产品序列号”文本框中键入 ISA Server 2006 的产品序列号。

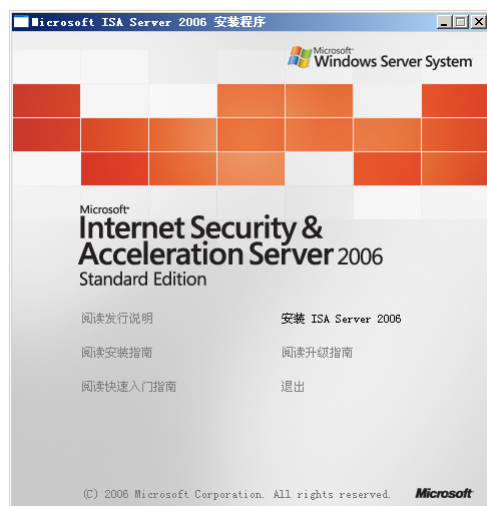


图 19-1 “Microsoft ISA Server 2006 安装程序”窗口

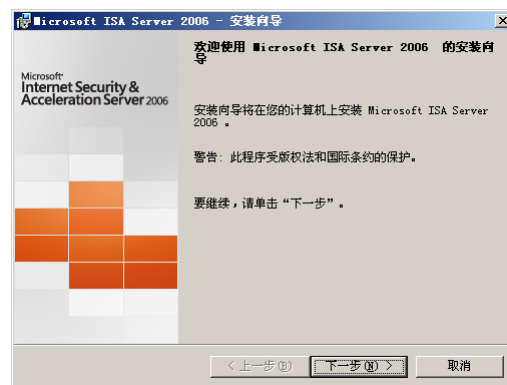


图 19-2 ISA Server 2006 安装向导



图 19-3 “许可协议”对话框



图 19-4 “客户信息”对话框

⑤ 单击“下一步”按钮，显示如图 19-5 所示的“安装类型”对话框。在其中选择安装类型，这里选择“自定义”单选按钮。

⑥ 单击“下一步”按钮，显示如图 19-6 所示的“自定义安装”对话框。在其中选择要安装的功能，并可更改安装路径。

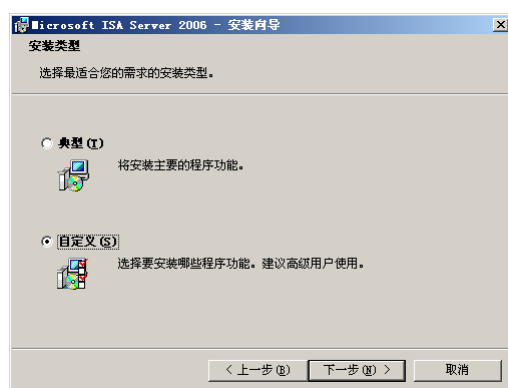


图 19-5 “安装类型”对话框

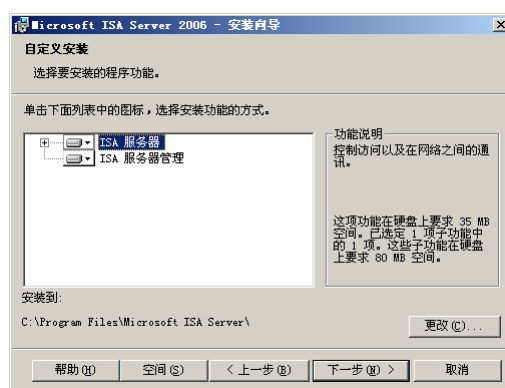


图 19-6 “自定义安装”对话框

⑦ 单击“下一步”按钮，显示如图 19-7 所示的“内部网络”对话框，在其中指定在 ISA 服务器内部网络中的地址范围。

⑧ 单击“添加”按钮，显示如图 19-8 所示的“地址”对话框，在其中添加在该网络中包括的 IP 地址范围。

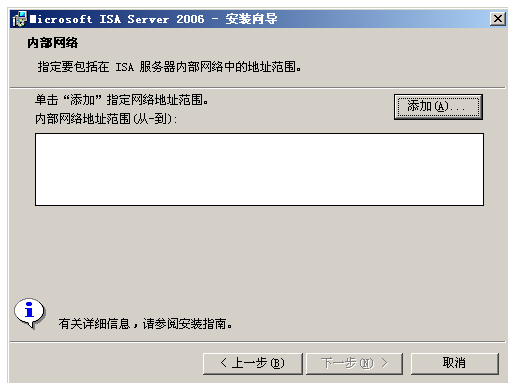


图 19-7 “内部网络”对话框

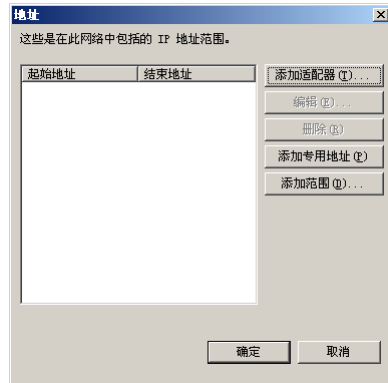


图 19-8 “地址”对话框

如果要根据网卡添加，则单击“添加适配器”按钮，显示如图 19-9 所示的“选择网络适配器”对话框。

如果要添加一个特定的 IP 地址范围，则单击“添加范围”按钮，显示如图 19-10 所示的“IP 地址范围属性”对话框，分别在“起始地址”和“结束地址”文本框中键入开始和结束 IP 地址即可。

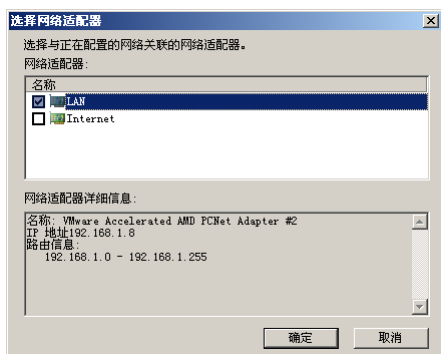


图 19-9 “选择网络适配器”对话框

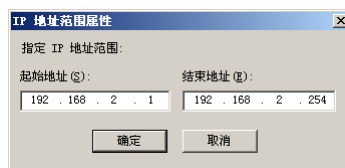


图 19-10 “IP 地址范围属性”对话框

⑨ 单击“确定”按钮返回“内部网络”对话框，其中显示所添加的 IP 地址范围，如图 19-11 所示。

⑩ 单击“下一步”按钮，显示如图 19-12 所示的“防火墙客户端连接”对话框，在其中指定是否接受来自不加密的防火墙客户端的连接。

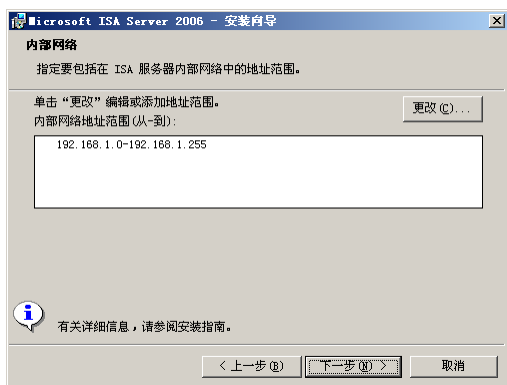


图 19-11 内部网络地址范围

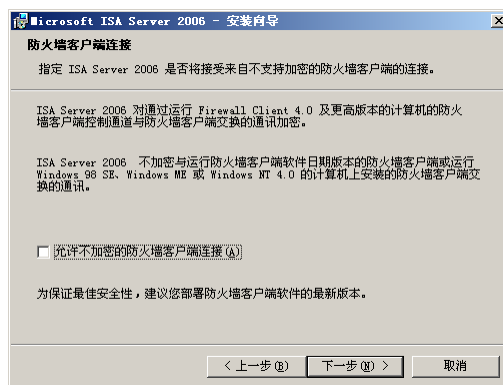


图 19-12 “防火墙客户端连接”对话框

⑪ 单击“下一步”按钮，显示如图 19-13 所示的“服务警告”对话框，其中提示在安装过程中，可能会被重新启动的服务。

⑫ 单击“下一步”按钮，显示如图 19-14 所示的“可以安装程序了”对话框。

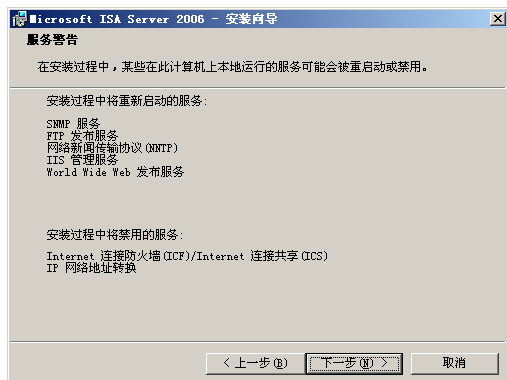


图 19-13 “服务警告”对话框

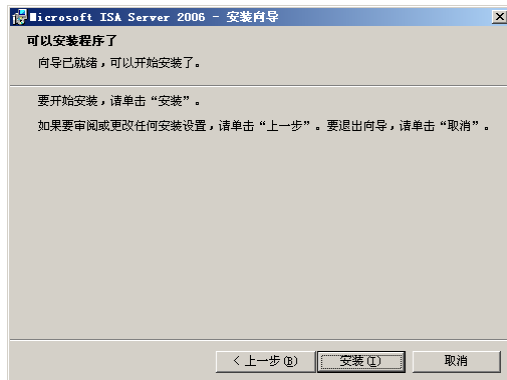


图 19-14 “可以安装程序了”对话框

⑬ 单击“安装”按钮，开始安装 ISA Server 2006，安装完成显示如图 19-15 所示的“安装向导完成”对话框。



图 19-15 “安装向导完成”对话框

⑭ 单击“完成”按钮，显示如图 19-16 所示的“保护 ISA 服务器的计算机”窗口，其中显示 ISA 服务器的一些说明信息。至此，ISA Server 2006 安装完成。

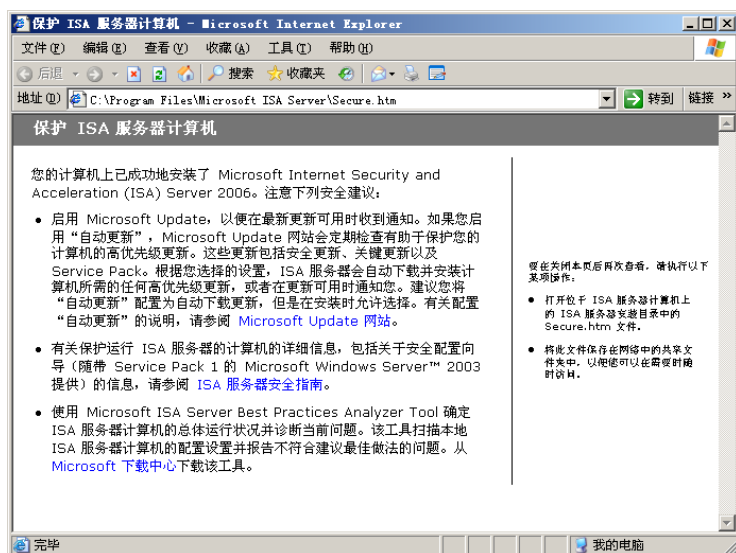


图 19-16 “保护 ISA 服务器的计算机”窗口

单击“开始”→“所有程序”→“Microsoft ISA Server”→“ISA 服务管理器”选项，显示 ISA 服务管理器控制台窗口，如图 19-17 所示，在其中可以配置 ISA Server。



图 19-17 ISA 服务管理器

19.4 实现安全 Internet 共享

ISA Server 2006 功能强大，设置和使用都很方便。它不仅将网络划分为内网和外网，还多了一个“本地主机”部分，从而进一步提高了 ISA Server 的安全性。默认情况下，ISA Server 2006 安装完成后会“隔离”内、外网，并禁止任何通过 ISA Server 的通信，任何未经明确“允许”的行为默认都是禁止的。

19.4.1 允许内网访问 Internet

由于 ISA Server 默认会禁止内网与外网的通信，因此如果网络中的用户想通过 ISA Server 连接到 Internet，必须创建一条规则允许内网用户访问 Internet。

① 在 ISA Server 2006 控制台中，在左窗格中选择“防火墙策略”选项。显示“防火墙策略”窗口，如图 19-18 所示。默认只有一个规则，拒绝所有网络的通信。

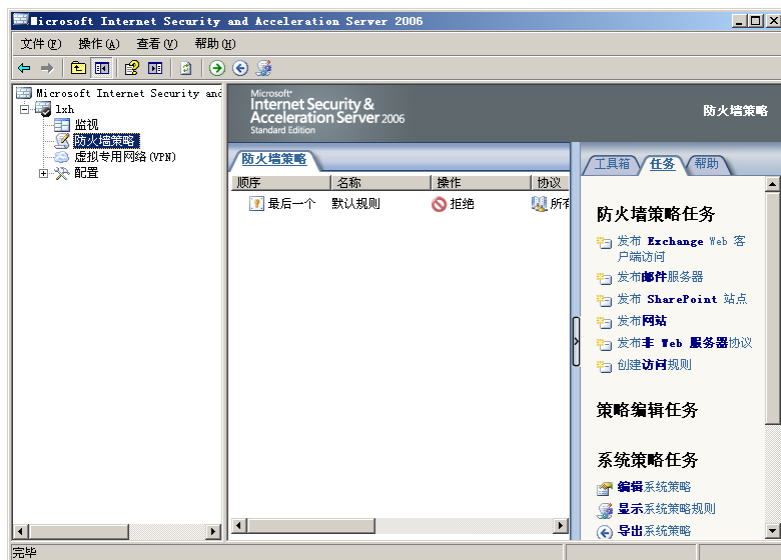


图 19-18 “防火墙策略”窗口

② 右击“防火墙策略”选项，在快捷菜单中选择“新建”→“访问规则”选项。打开“新建访问规则向导”对话框，如图 19-19 所示。在“访问规则名称”文本框中为新规则设置一个名称，例如“允许内网访问 Internet”。



提示

由于在设置 ISA Server 时需要创建多个访问规则，因此为了便于识别各条规则，应为其设置容易识别的名称。

③ 单击“下一步”按钮，显示如图 19-20 所示的“规则操作”对话框，选择“允许”单选按钮。

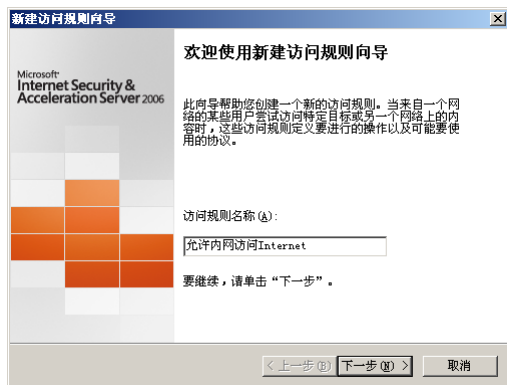


图 19-19 “新建访问规则向导”对话框

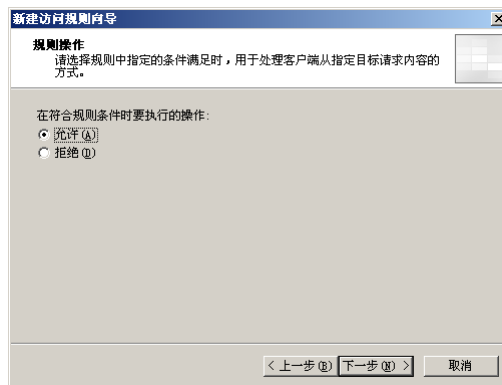


图 19-20 “规则操作”对话框

④ 单击“下一步”按钮，显示如图 19-21 所示的“协议”对话框。在其中选择创建该规则使用的协议，包括“所有出站通信”、“所选协议”和“选择以外所有出站协议”。如果选择“所有出站通信”选项，则允许所有的协议，相当于防火墙不起作用，因此这里选择“所选的协议”选项。

⑤ 单击“添加”按钮，显示“添加协议”对话框。展开“通用协议”选项，分别双击“DNS”、“HTTP”、“HTTPS”、“POP3”和“SMTP”选项，将其添加到“协议”列表框中。展开“Web”，双击添加“FTP”，如图 19-22 所示。

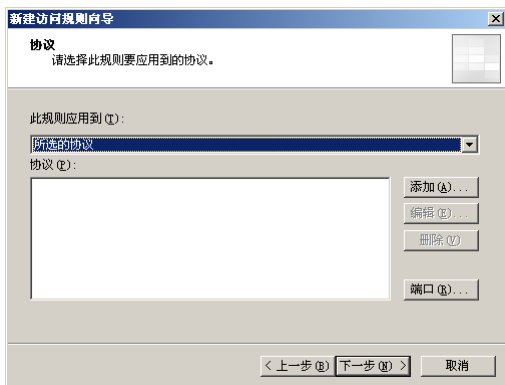


图 19-21 “协议”对话框



图 19-22 添加协议

⑥ 单击“关闭”按钮，添加完成协议，如图 19-23 所示。

⑦ 单击“下一步”按钮，显示如图 19-24 所示的“访问规则源”对话框，在其中选择通信的方向。

⑧ 单击“添加”按钮，显示“添加网络实体”对话框。因为要创建内部访问 Internet 的规则，因此展开“网络”选项，双击添加“内部”选项。如果要使 ISA 服务器也能访问 Internet，还应添加“本地主机”，如图 19-25 所示。单击“关闭”按钮关闭。

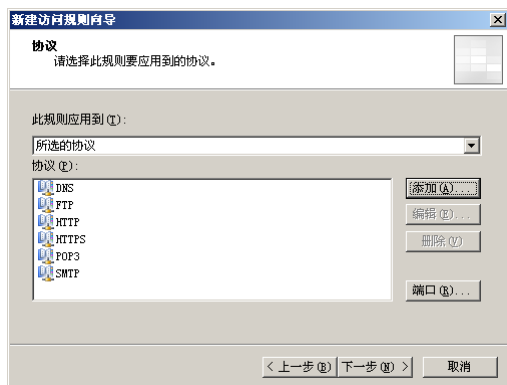


图 19-23 添加完成协议

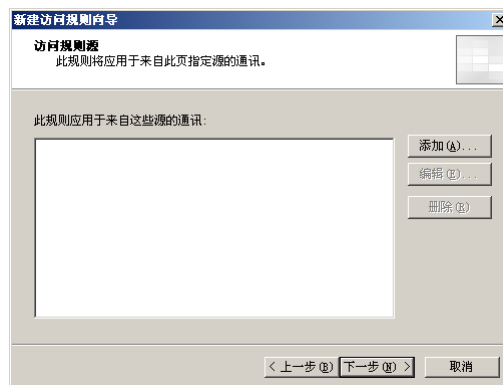


图 19-24 “访问规则源”对话框

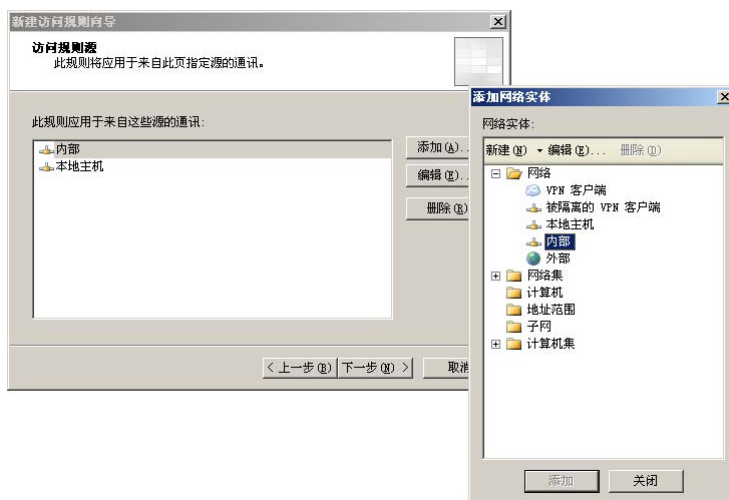


图 19-25 添加网络实体

⑨ 单击“下一步”按钮，显示如图 19-26 所示的“访问规则目标”对话框。单击“添加”按钮，显示“添加网络实体”对话框。展开“网络”选项，双击添加“外部”。



图 19-26 “访问规则目标”对话框

⑩ 单击“下一步”按钮，显示如图 19-27 所示的“用户集”对话框，保留默认设置即可。

⑪ 单击“下一步”按钮，显示如图 19-28 所示的“正在完成新建访问规则向导”对话框。

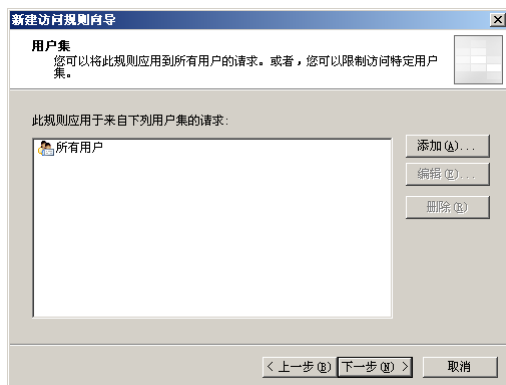


图 19-27 “用户集”对话框



图 19-28 “正在完成新建访问规则向导”对话框

⑫ 单击“完成”按钮，规则创建完成。显示在 ISA Server 2006 控制台中，如图 19-29 所示。不过，新创建的规则并不会立即生效。

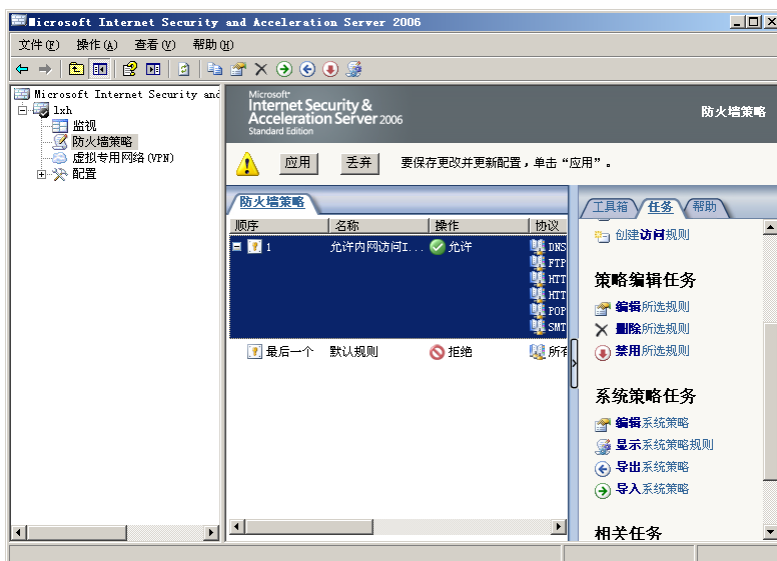


图 19-29 创建完成的规则

⑬ 单击“应用”按钮，显示如图 19-30 所示的“正在保存配置更改”对话框。提示应用新规则，单击“确定”按钮即可。



图 19-30 “正在保存配置更改”对话框

新规则生效以后，来自局域网的计算机即可通过 ISA Server 访问 Internet。不过，用户在访问 Internet 中 FTP 服务器时只能读取文件，而不能上传文件。为了能使 FTP 协议上传文件，应执行以下操作。

选择刚刚创建的规则，右击并从快捷菜单中选择“配置 FTP”选项，显示如图 19-31 所示的“配置 FTP 协议策略”对话框。清除“只读”复选框，单击“确定”按钮，然后在 ISA Server 控制台中应用配置。

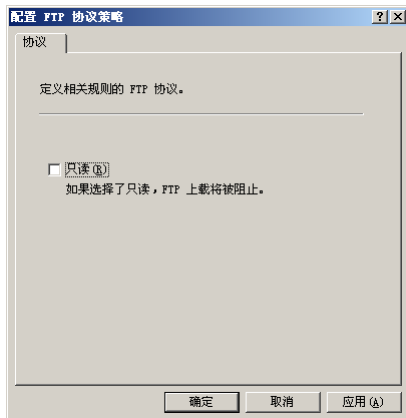


图 19-31 “配置 FTP 协议策略”对话框

19.4.2 允许内网 ping 通网关

在网络出现故障时，利用 Ping 命令检查是网络管理员常用的方式。当计算机通过 ISA Server 服务器访问网络时，ISA Server 2006 就是网关。不过默认情况下，内部网络的计算机不能 Ping 通 ISA Server 服务器，因此需要创建一条规则允许内网计算机 ping 通 ISA Server 2006 服务及外网。

① 在 ISA Server 2006 控制台的“防火墙策略”窗口中单击“创建新的访问规则”选项，打开如图 19-32 所示的“新建访问规则向导”对话框。在“访问规则名称”文本框中键入网关，例如“允许内网 Ping 通网关”。

② 单击“下一步”按钮，显示如图 19-33 所示的“规则操作”对话框，选择“允许”单选按钮。

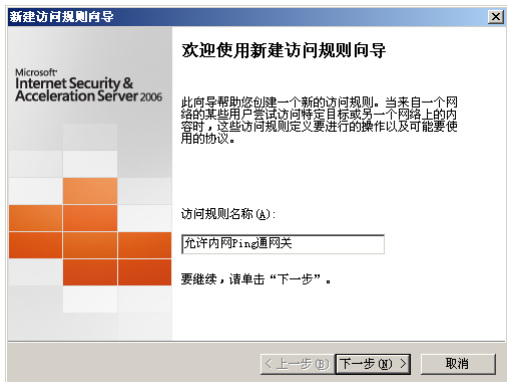


图 19-32 “新建访问规则向导”对话框

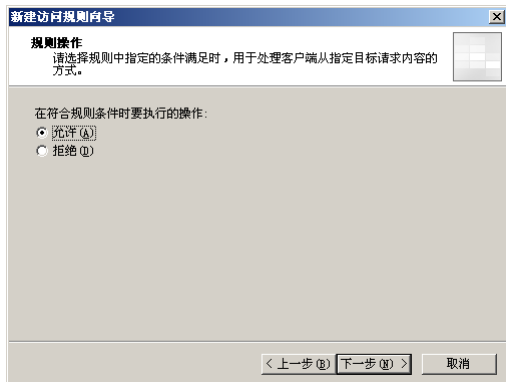


图 19-33 “规则操作”对话框

③ 单击“下一步”按钮，显示“协议”对话框。在“此规则应用到”下拉列表框中选择“所选的协议”选项，单击“添加”按钮，打开“添加协议”对话框。展开“结构”选项，双击添加“PING”，如图 19-34 所示，然后单击“关闭”按钮返回。

④ 单击“下一步”按钮，显示“访问规则源”对话框。单击“添加”按钮，显示“添加网络实体”对话框。展开“网络”选项，双击添加“内部”，如图 19-35 所示，然后单击“关闭”按钮返回。

⑤ 单击“下一步”按钮，显示“访问规则目标”对话框。单击“添加”按钮，显示“添加网络实体”对话框，添加“本地主机”和“外部”，如图 19-36 所示。

⑥ 单击“下一步”按钮，显示“用户集”对话框。

⑦ 单击“下一步”按钮，显示“正在完成新建访问规则向导”对话框。单击“完成”按钮，创建完成规则。

⑧ 在 ISA Server 控制台窗口中单击“应用”按钮使配置生效。

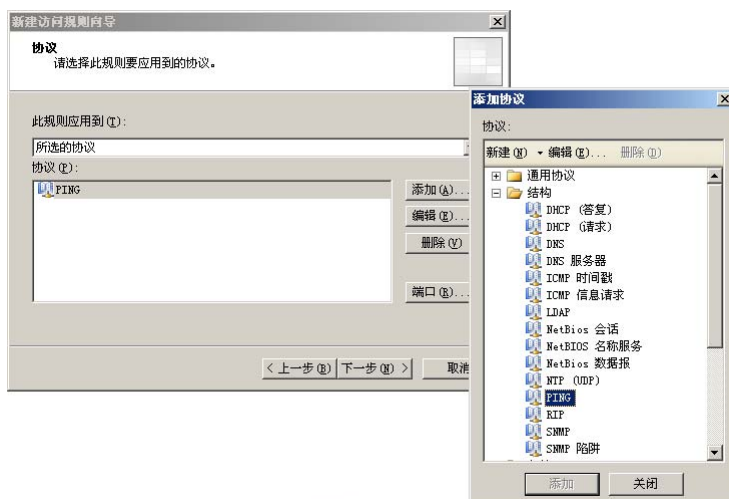


图 19-34 添加 ping 协议

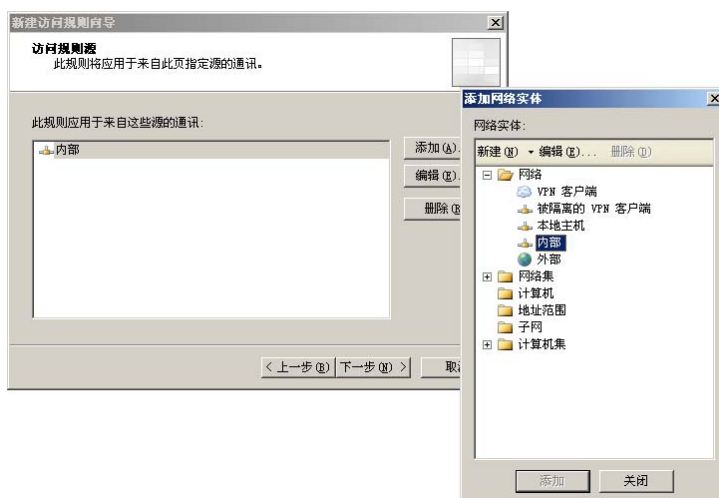


图 19-35 添加内部

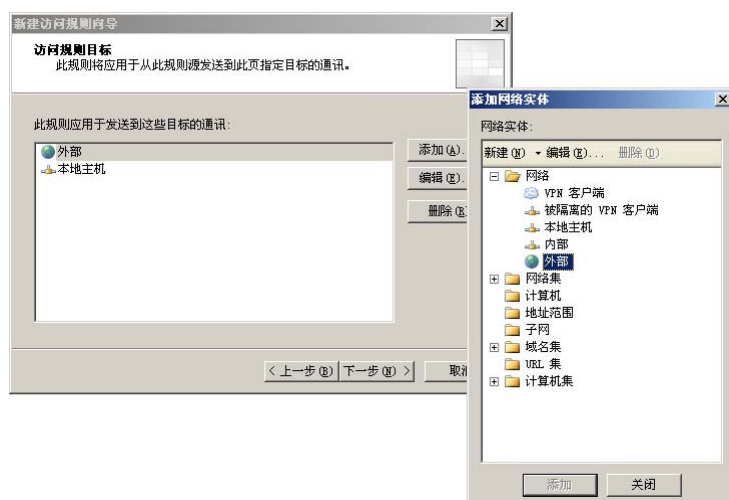


图 19-36 添加本地主机和外部

19.4.3 设置 Internet 访问限制

随着网络的盛行，大部分人都喜欢使用即时消息软件进行交流。不过在企业中却往往禁止用户在

上班时使用这些软件,以免影响正常工作。在 ISA Server 2006 中,默认提供了 AOL、ICQ、IRC、Net2Phone 及 MSN Messenger 等软件的协议。而未提供一些国内即时通信软件,例如 QQ 及 UC 等,不过可以由用户手动添加。

1. 添加 QQ 协议

QQ 的服务器端默认使用 UDP 协议的 4000~4001 和 8000 端口,添加 QQ 协议就是添加这些端口的“协议”。

① 打开 ISA Server 2006 控制台,在右侧下拉列表框中选择“工具箱”选项并选择“协议”选项组,如图 19-37 所示。

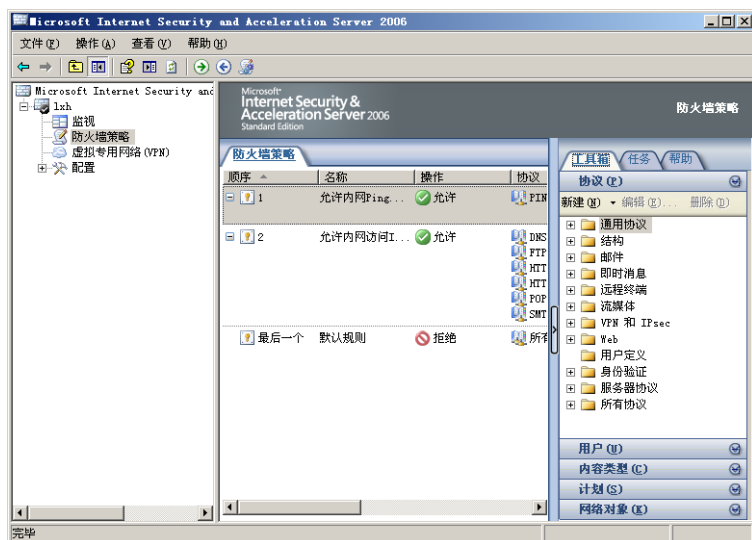


图 19-37 选“协议”选项组

② 单击“新建”按钮,选择下拉菜单中的“协议”选项,打开图 19-38 所示的“新建协议定义向导”对话框。在“协议定义名称”文本框中键入名称,如 QQ。

③ 单击“下一步”按钮,显示如图 19-39 所示的“首要连接信息”对话框,在其中设置端口号和协议。

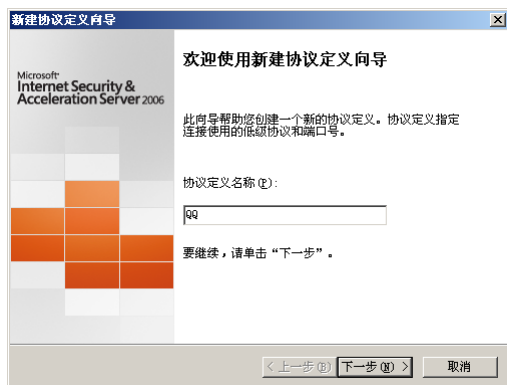


图 19-38 “新建协议定义向导”对话框



图 19-39 新建连接信息

④ 单击“新建”按钮,显示如图 19-40 所示的“新建/编辑协议连接”对话框。在“协议类型”下拉列表框中选择“UDP”选项,在“方向”下拉列表框中选择“发送接收”选项。在“端口范围”文本框中分别键入 4000 和 4010。

⑤ 单击“确定”按钮,然后次单击“新建”按钮,添加端口范围为 8000 的“UDP”协议,如图 19-41 所示。



图 19-40 “新建/编辑协议连接”对话框

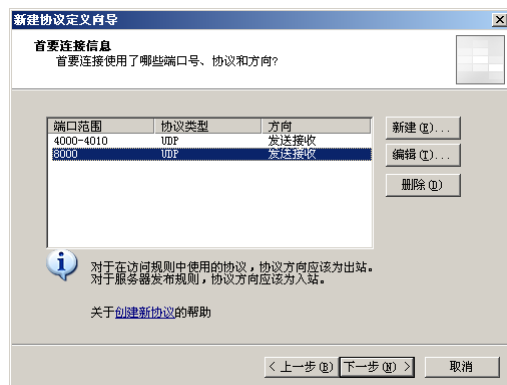


图 19-41 添加端口范围

- ⑥ 单击“下一步”按钮，显示如图 19-42 所示的“辅助连接”对话框，选择“否”单选按钮。
- ⑦ 单击“下一步”按钮，显示如图 19-43 所示的“正在完成新建协议定义向导”对话框。

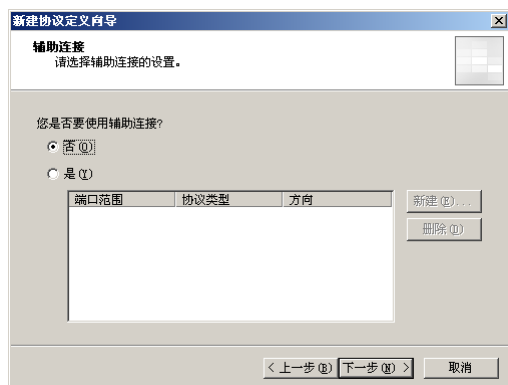


图 19-42 “辅助连接”对话框

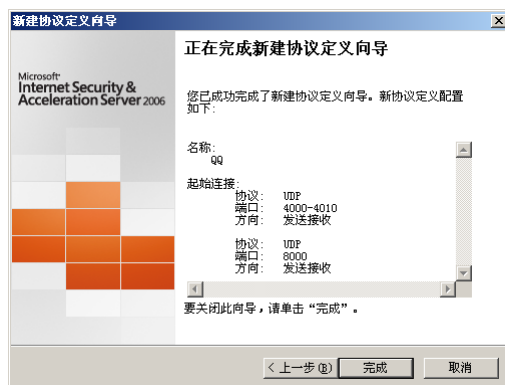


图 19-43 “正在完成新建协议定义向导”对话框

- ⑧ 单击“完成”按钮，QQ 协议添加完成。

2. 添加 UC 协议

UC 使用 TCP 和 UDP 两种协议，应添加 UC 协议并且使用 TCP 协议端口为 3001 和 3002 的出站连接，以及 UDP 协议端口为 3001 和 3002 的发送接收连接。

- ① 运行“新建协议定义向导”，在“首要连接信息”对话框中添加“协议类型”为 TCP、“方向”为“出站”，以及“端口范围”为 3000 和 3002 的协议连接，如图 19-44 所示。
- ② 添加一个“协议类型”为 UDP、“方向”为“发送接收”，以及“端口范围”为 3000 和 3002 的协议连接，如图 19-45 所示。



图 19-44 添加 UC 协议连接



图 19-45 添加 UDP 协议的协议连接

- ③ 添加完成以后，显示“首要连接信息”对话框，如图 19-46 所示。其他操作步骤和添加 QQ 协议相同，这里不再赘述。



图 19-46 “首要连接信息”对话框

添加成功用户自定义的协议后，这些协议显示在“用户定义”下拉列表框中，如图 19-47 所示。在添加 ISA Server 规则时，可以选择添加这些协议。

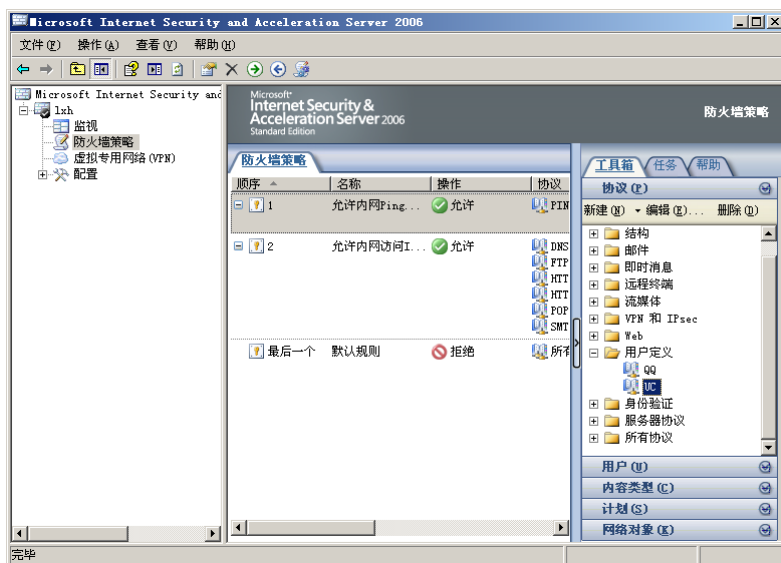


图 19-47 添加成功的协议

3. 添加访问规则

如果要限制内网用户使用 QQ 及 UC 等即时通信软件，可以添加一条规则拒绝内部用户使用 QQ 和 UC 协议。

- ① 运行“新建访问规则向导”在如图 19-48 所示的“规则操作”对话框中选择“拒绝”单选按钮。

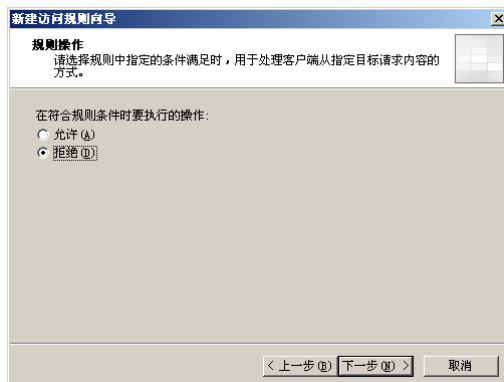


图 19-48 “规则操作”对话框

- ② 当显示“协议”对话框时，添加“用户自定义”中的 QQ 和 UC 协议，如图 19-49 所示。

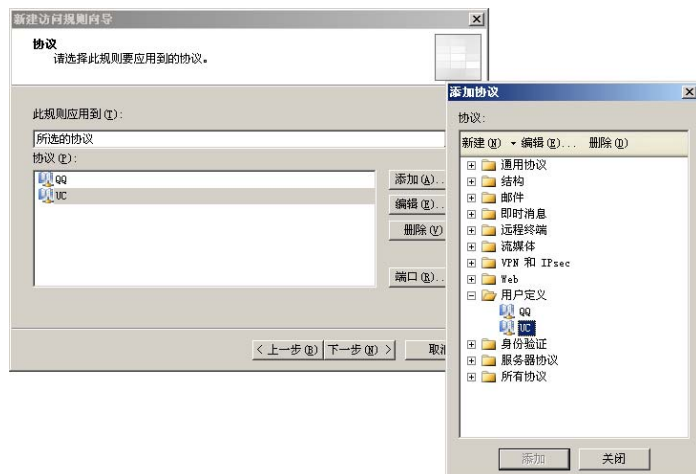


图 19-49 添加 QQ 和 UC 协议

- ③ 在“访问规则源”对话框中单击“添加”按钮添加“内部”。
- ④ 在“访问规则目标”对话框中，单击“添加”按钮添加“外部”。
- ⑤ 创建完成规则以后，即可设置用户的限制时间。右击该规则并选择快捷菜单中的“属性”选项，显示如图 19-50 所示的属性对话框。
- ⑥ 打开“计划”选项卡，如图 19-51 所示，在其中设置用户的活动时间。

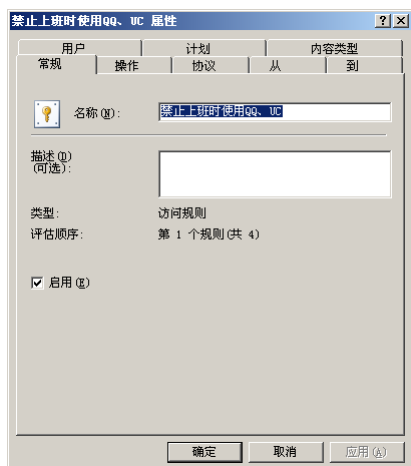


图 19-50 属性对话框

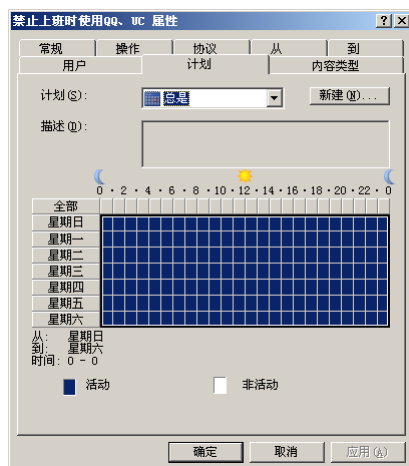


图 19-51 “计划”选项卡

⑦ 单击“新建”按钮，显示“新建计划”对话框。在“名称”文本框设置一个名称，然后将所有时间设置为“非活动”。将星期一~星期五的上午 8 点~下午 18 点之间设置为“活动”，即该规则只在活动时间内有效，如图 19-52 所示。

⑧ 依次单击“确定”按钮保存，并单击“应用”按钮使设置生效。这样在规则活动时间内，用户将不能使用 QQ 和 UC 软件。

19.4.4 设置屏蔽网站

Internet 上的信息浩如烟海，在提供便利的同时也有一些网站存在不良信息和带有恶意代码的网站。在 ISA Server 中可以通

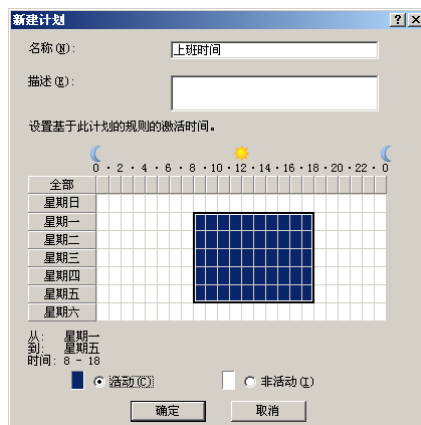


图 19-52 设置计划时间

过添加规则来屏蔽这些站点。不过，由于除了使用 HTTP 协议的 Web 网站，还有其他使用 FTP 及 telnet 等协议的网站，因此需要添加所有有关的协议。

- (1) 在 ISA Server 2006 控制台中启动“新建访问规则向导”。
- (2) 在“规则操作”对话框中选择“拒绝”单选按钮。
- (3) 在如图 19-53 所示的“协议”对话框中，选择“所有出站通信”选项。
- (4) 在“访问规则源”中添加“内部”和“本地主机”，如图 19-54 所示。

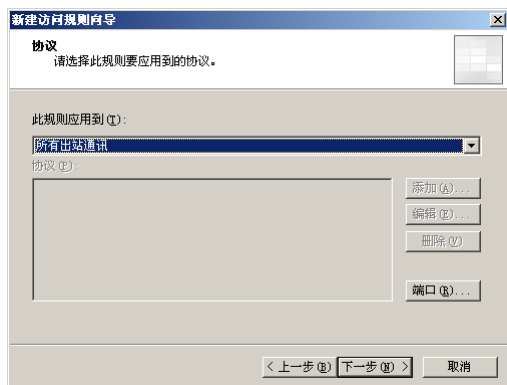


图 19-53 “协议”对话框



图 19-54 添加“内部”和“本地主机”

(5) 在“访问规则目标”对话框中单击“添加”按钮打开“添加网络实体”对话框。单击“新建”按钮，选择“URL 集”选项，显示如图 19-55 所示的“新建 URL 集规则元素”对话框。在“名称”文本框中设置一个名称，然后单击“新建”按钮。按照“http://*.xxx.zzz/*”的格式添加被禁止的网站，单击“确定”按钮保存。

(6) 添加其他协议的“域名集”，在“添加网络实体”对话框中单击“新建”→“域名集”选项，显示如图 19-56 所示的“新建域名集策略元素”对话框。在“名称”文本框中设置一个名称，单击“新建”按钮，添加被禁止的域名，如*.xxx.com。

(7) 添加完成域名集和 URL 集之后，将其添加到“访问规则目标”对话框中，如图 19-57 所示。

(8) 单击“下一步”按钮，直至规则添加完成，然后单击“应用”按钮使配置生效即可。

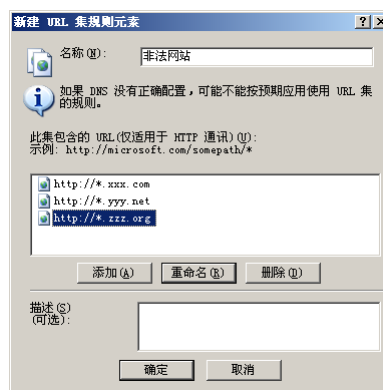


图 19-55 “新建 URL 集规则元素”对话框

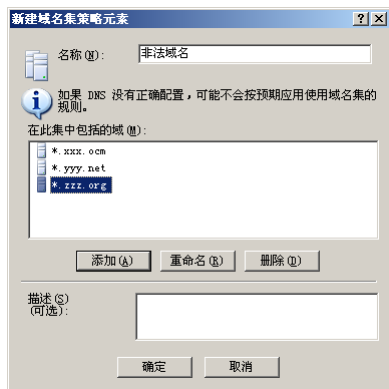


图 19-56 “新建域名集策略元素”对话框



图 19-57 添加自定义域名集和 URL 集

19.4.5 设置阻止文件类型

使用 HTTP 过滤器还可以根据文件的扩展名进行限制。例如，需禁止当前网页运行某些控件，以防止木马或病毒，或者想禁止运行 Flash 动画，或者不希望网页中出现 BT 种子文件扩展名等都可以通过阻止文件扩展名来实现。

(1) 在“防火墙策略”窗口中选择已创建的“允许内网计算机访问 Internet”规则，右击并从快捷菜单中选择“配置 HTTP”选项，打开“为规则配置 HTTP 策略”对话框。打开如图 19-58 所示的“扩展名”选项卡，在“指定对文件扩展名要执行的操作”下拉列表框中选择“阻止指定的扩展名（允许所有其他扩展名）”选项。

(2) 单击“添加”按钮，显示“扩展名”对话框。在“扩展名”文本框中键入需要阻止的扩展名，在“描述”文本框中键入说明信息，如图 19-59 所示。

(3) 单击“确定”按钮，添加成功一个扩展名。按照同样操作步骤，可以添加多种扩展名，如图 19-60 所示。

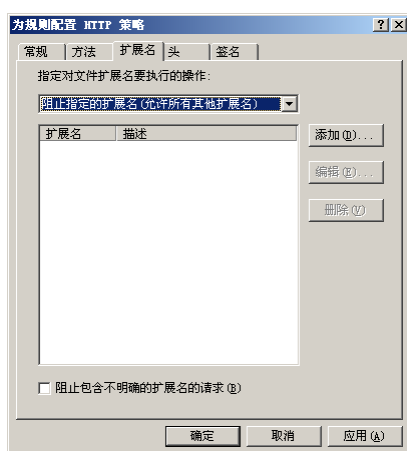


图 19-58 “扩展名”选项中

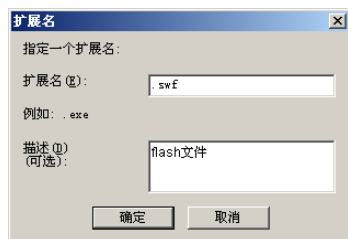


图 19-59 添加扩展名及说明信息

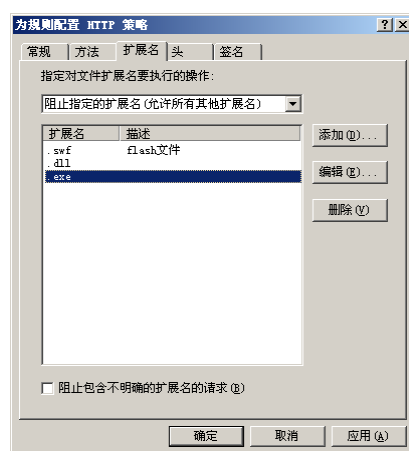


图 19-60 添加扩展名

(4) 单击“确定”按钮保存设置，并应用设置使其生效即可。

19.4.6 设置用户分组与权限

在 ISA Server 服务器中可以为不同的用户为不同用户分配不同的访问权限的操作步骤如下，以便更好地控制和管理 ISA Server。在 ISA 服务器中可为用户及组分配以下权限。

- ISA 服务器阵列管理员：具有对 ISA 阵列的完全控制权限。还可以查看应用于阵列的企业策略。
- ISA 服务器阵列审核员：具有监视权限并可查看阵列配置。
- ISA 服务器阵列监视审核员：具有某些监视权限。

(1) 在 ISA Server 2006 控制台展开左窗格中的“配置”选项。选择“常规”选项，显示的“常规”窗口如图 19-61 所示。

(2) 单击“分配管理角色”选项，在显示的对话框中打开如图 19-62 所示的“分配角色”选项卡。默认情况下，只有用户账户 Administrator 和用户组 Administrators，并且均具有“ISA 服务器完全权限管理员”权限。

(3) 如果要为其他用户分配权限，则可单击“添加”按钮，显示如图 19-63 所示的“管理委派”对话框。在“组或用户”文本框中单击“浏览”按钮，选择要指定权限的用户或组，在“角色”下拉列表框中选择要分配的权限。



图 19-61 “常规”窗口

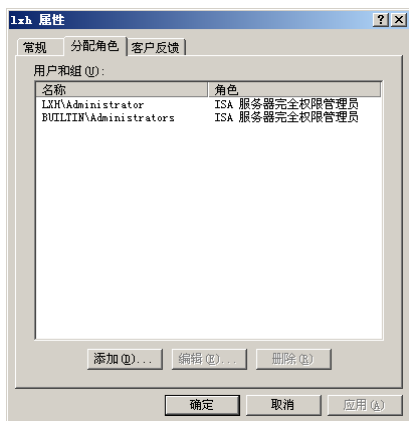


图 19-62 “分配角色”选项卡

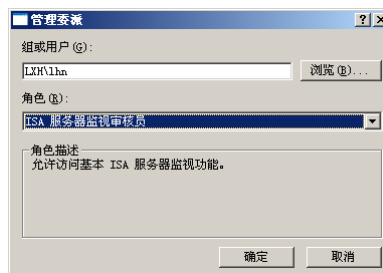


图 19-63 “管理委派”对话框

(4) 单击“确定”按钮，添加完成用户或组。单击“确定”按钮返回 ISA Server 控制台，单击“应用”按钮应用所做的设置即可。

19.5 发布内部服务器

默认情况下，内部网络的所有服务器都受 ISA Server 服务器保护，外网用户无法访问到这些服务器。不过企业网络通常需要搭建一些服务器为 Internet 提供服务，如 Web 及 Email 服务器等，此时需要利用 ISA Server 将服务器发布到 Internet。

19.5.1 发布 Web 站点

利用 ISA Server 2006 的“网站发布规则”可以将网络中的 Web 网站发布到 Internet。

① 在 ISA Server 2006 控制台中右击“防火墙策略”选项，在快捷菜单中选择“新建”→“网站发布规则”选项。打开如图 19-64 所示的“新建 Web 发布规则向导”对话框，在“Web 发布规则名称”文本框中为新规则设置一个名称。

② 单击“下一步”按钮，显示如图 19-65 所示的“请选择规则操作”对话框，选择“允许”单选按钮。

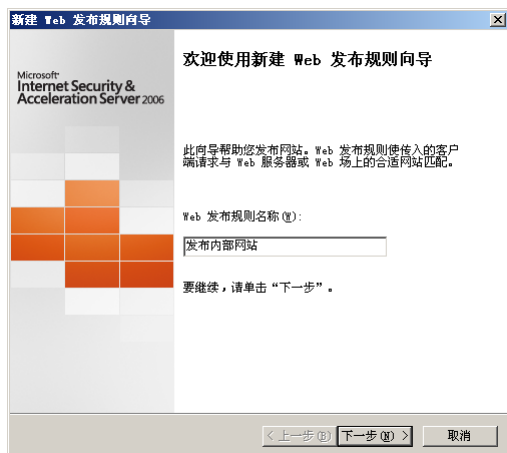


图 19-64 “新建 Web 发布规则向导”对话框

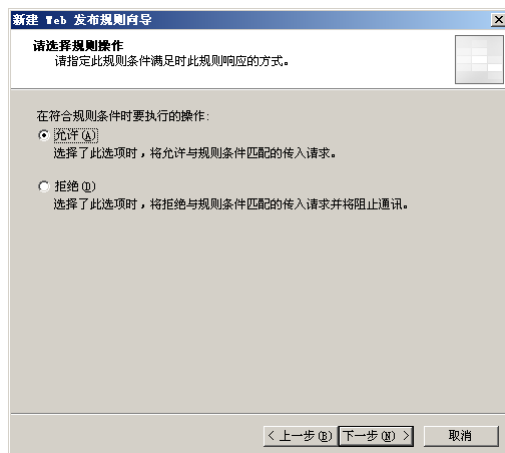


图 19-65 “请选择规则操作”对话框

③ 单击“下一步”按钮，显示如图 19-66 所示的“发布类型”对话框。如果只发布一个网站或一个网站的群集服务器，则选择“发布单个网站或负载均衡器”单选按钮，这里选择该单选按钮；如果发布 Web 服务器上的多个站点，则选择“发布多个网站”单选按钮。

④ 单击“下一步”按钮，显示如图 19-67 所示的“服务器连接安全”对话框，选择“使用不安全的连接发布的 Web 服务器或服务器场”单选按钮。

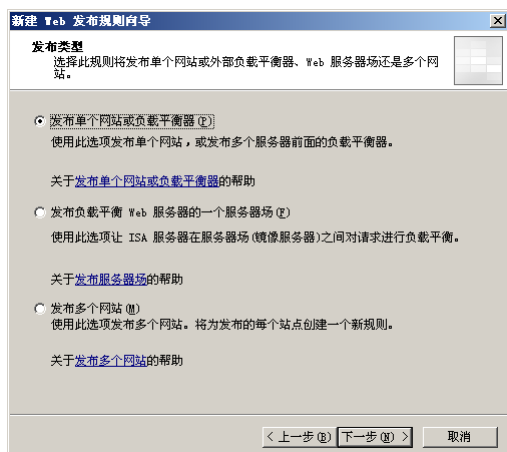


图 19-66 “发布类型”对话框

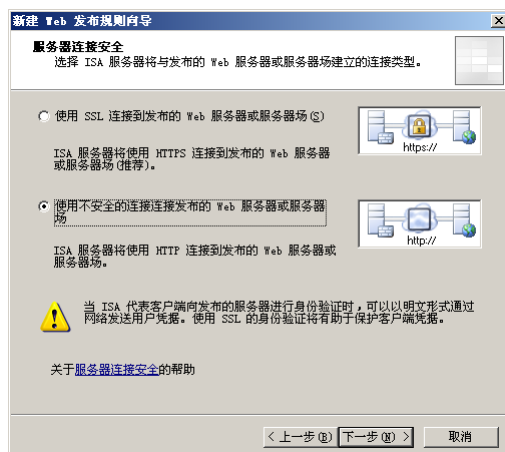


图 19-67 “服务器连接安全”对话框

⑤ 单击“下一步”按钮，显示如图 19-68 所示的“内部发布详细信息”对话框。在“内部站点名称”文本框中键入网站域名，如 www.coolpen.net。选中“使用计算机名称或 IP 地址连接到发布的服务器”复选框，在“计算机名称或 IP 地址”文本框中键入 Web 服务器的计算机名或 IP 地址。

⑥ 单击“下一步”按钮，显示如图 19-69 所示的“内部发布详细信息”对话框，在“路径”文本框中键入“/*”。

⑦ 单击“下一步”按钮，显示如图 19-70 所示的“公共名称细节”对话框，在“公用名称”文本框中键入发布到 Internet 上的名称。

⑧ 单击“下一步”按钮，显示如图 19-71 所示的“选择 Web 侦听器”对话框，在其中为发布的站点选择 Web 侦听器。在 ISA Server 中每个绑定的 IP 地址（通常是 Internet 地址）都可以创建一个 Web 侦听器，并且选择该侦听器作为发布地址。默认情况下没有 Web 侦听器。

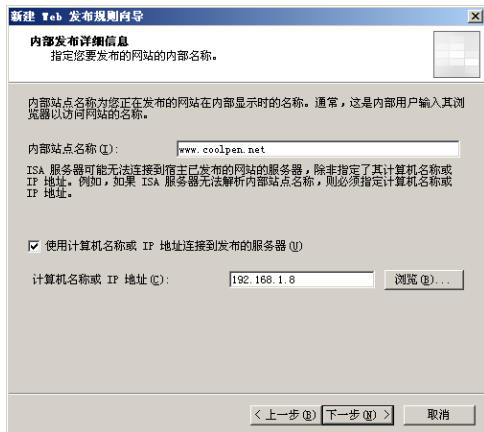


图 19-68 “内部发布详细信息”对话框

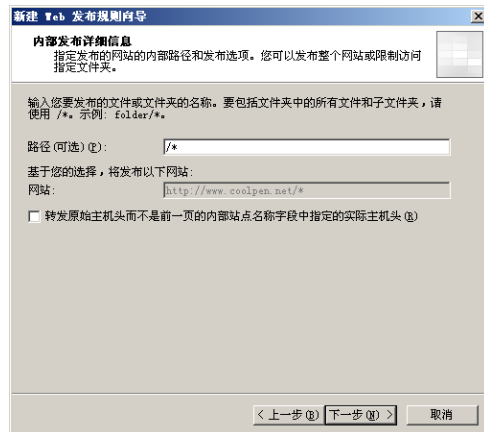


图 19-69 “内部发布详细信息”对话框

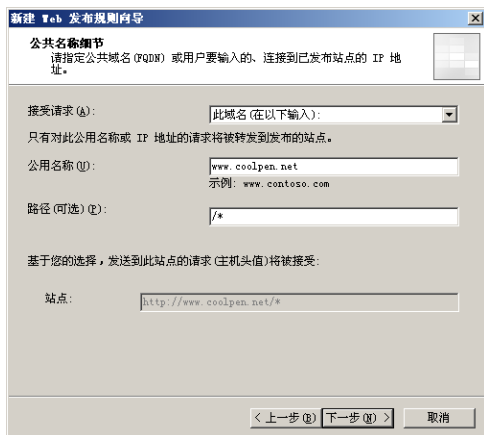


图 19-70 “公共名称细节”对话框

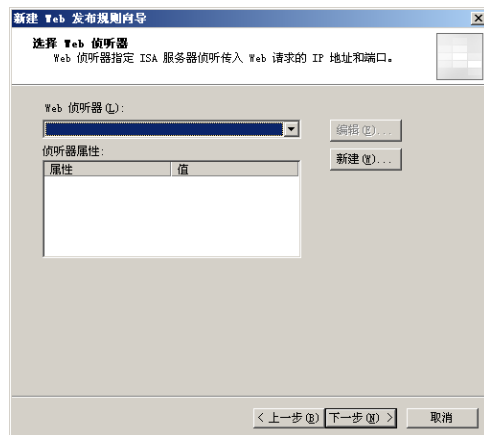


图 19-71 “选择 Web 侦听器”对话框

⑨ 单击“新建”按钮，打开如图 19-72 所示的“新建 Web 侦听器定义向导”对话框，在“Web 侦听器名称”文本框中键入一个名称。

⑩ 单击“下一步”按钮，显示如图 19-73 所示的“客户端连接安全设置”对话框，选择“不需要与客户端建立 SSL 安全连接”单选按钮。

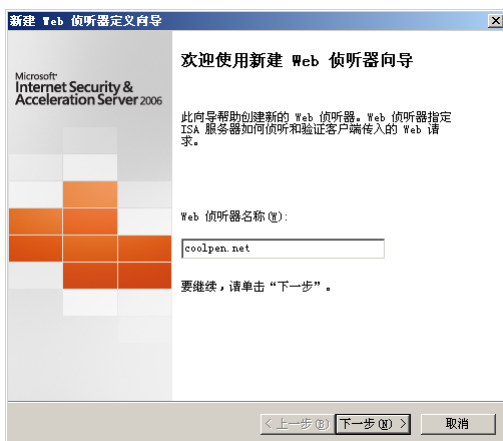


图 19-72 “新建 Web 侦听器定义向导”对话框

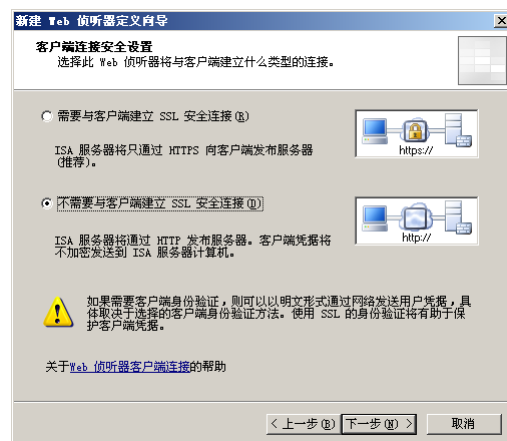


图 19-73 “客户端连接安全设置”对话框

⑪ 单击“下一步”按钮，显示如图 19-74 所示的“Web 侦听器 IP 地址”对话框，选择传入 Web 请求的网络并选中“外部”复选框。

⑫ 单击“下一步”按钮，显示如图 19-75 所示的“身份验证设置”对话框，在“选择客户端将

如何向 ISA 服务器提供凭据”下拉列表框中选择“没有身份验证”选项。

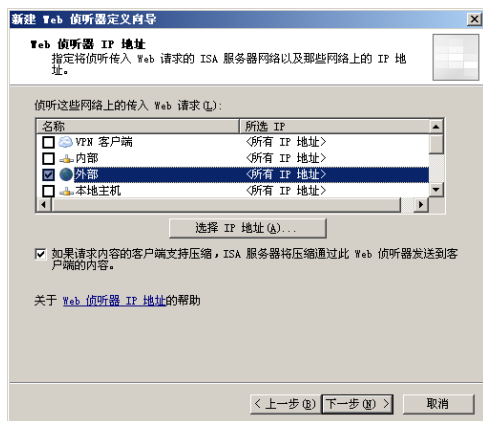


图 19-74 “Web 侦听器 IP 地址”对话框

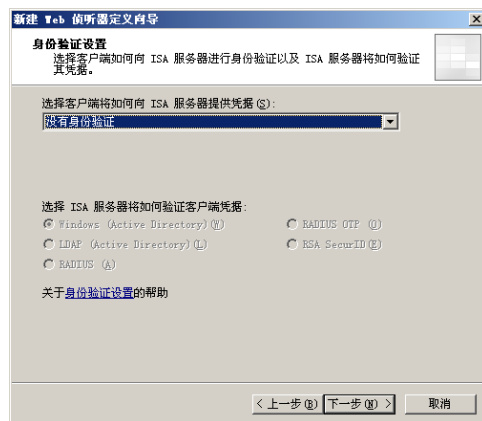


图 19-75 “身份验证设置”对话框

13 单击“下一步”按钮，显示如图 19-76 所示的“单一登录设置”对话框。

14 单击“下一步”按钮，显示如图 19-77 所示的“正在完成新建 Web 侦听器向导”对话框，表示 Web 侦听器已完成。

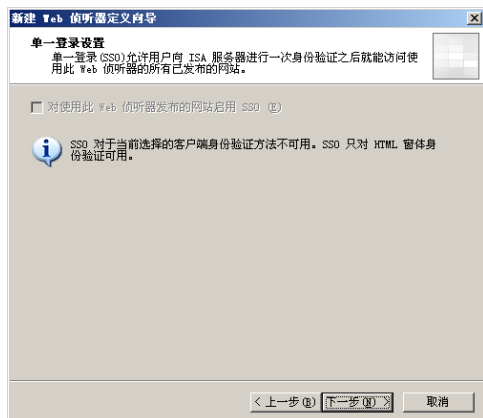


图 19-76 “单一登录设置”对话框



图 19-77 “正在完成新建 Web 侦听器向导”对话框

15 单击“完成”按钮返回“选择 Web 侦听器”对话框，在“Web 侦听器”下拉列表框中选择 Web 侦听器，如图 19-78 所示。

16 单击“下一步”按钮，显示如图 19-79 所示的“身份验证委派”对话框，在下拉列表框中选择“无委派，客户端无法直接进行身份验证”选项。

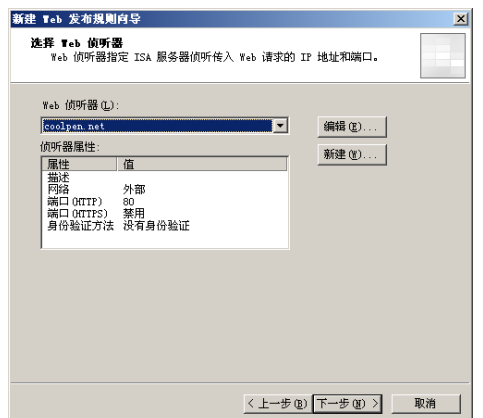


图 19-78 选择 Web 侦听器

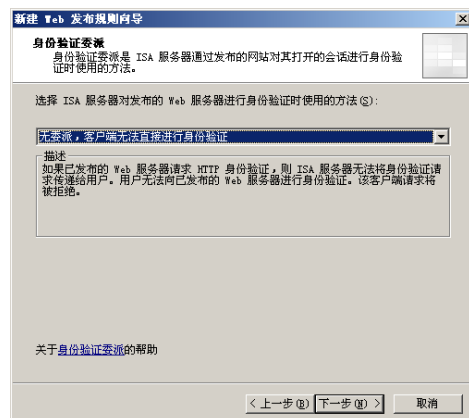


图 19-79 “身份验证委派”对话框

- ⑰ 单击“下一步”按钮，显示如图 19-80 所示的“用户集”对话框，使用默认设置即可。
- ⑱ 单击“下一步”按钮，显示如图 19-81 所示的“正在完成新建 Web 发布规则向导”对话框。



图 19-80 “用户集”对话框

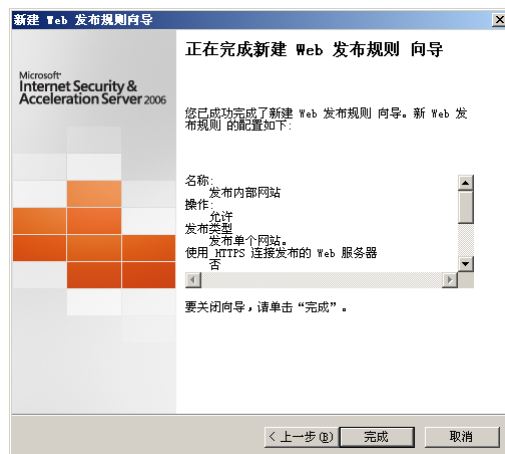


图 19-81 “正在完成新建 Web 发布规则向导”对话框

- ⑲ 单击“完成”按钮，创建完成 Web 发布规则，单击“应用”按钮使配置生效即可。

19.5.2 发布邮件服务器

利用 ISA Server 2006 的“邮件服务器发布规则”可以将使用 SMTP、RPC、POP、IMAP 和 NNTP 协议的邮件服务器发布到 Internet。

- ① 在 ISA Server 2006 控制台中右击“防火墙策略”选项，在快捷菜单中选择“新建”→“邮件服务器发布规则”选项。打开如图 19-82 所示的“新建邮件服务器发布规则向导”对话框，在“邮件服务器发布规则名称”文本框中键入一个名称。
- ② 单击“下一步”按钮，显示如图 19-83 所示的“选择访问类型”对话框，选择“客户端访问：RPC、IMAP、POP3、SMTP”单选按钮。

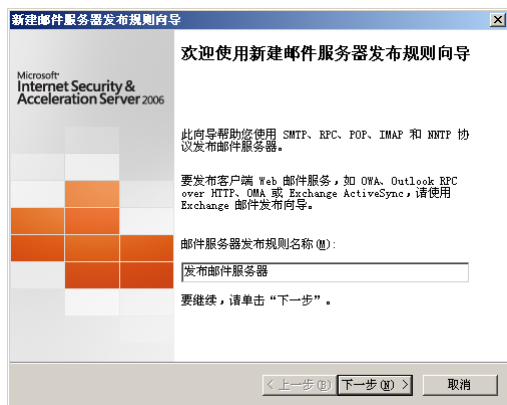


图 19-82 “新建邮件服务器发布规则向导”对话框

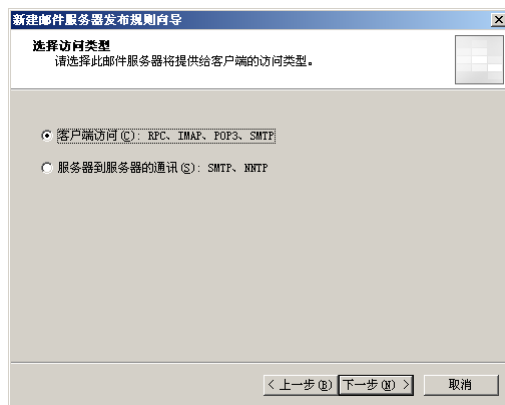


图 19-83 “选择访问类型”对话框

- ③ 单击“下一步”按钮，显示如图 19-84 所示的“选择服务”对话框，选中“POP3”和“SMTP”复选框。
- ④ 单击“下一步”按钮，显示如图 19-85 所示的“选择服务器”对话框，在“服务器 IP 地址”文本框中键入要发布的内网邮件服务器的 IP 地址。
- ⑤ 单击“下一步”按钮，显示如图 19-86 所示的“网络侦听器 IP 地址”对话框，选择“外部”复选框。
- ⑥ 单击“下一步”按钮，显示如图 19-87 所示的“正在完成新建邮件服务器发布规则向导”对话框。

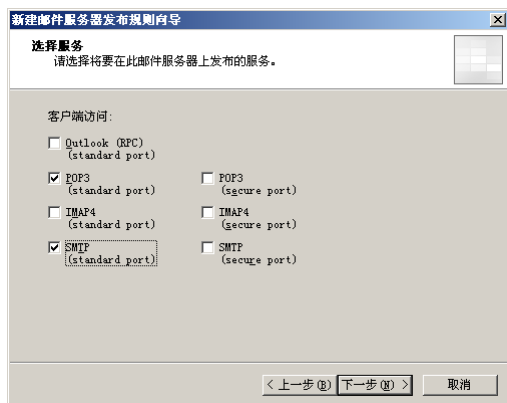


图 19-84 “选择服务”对话框

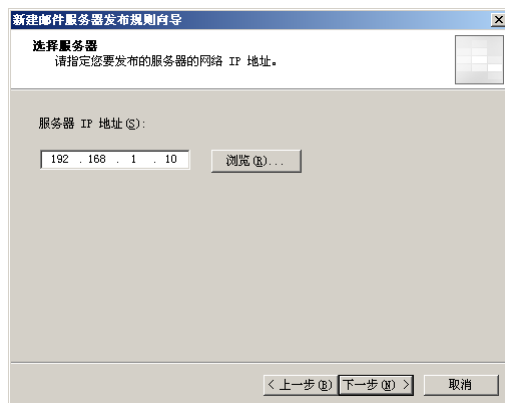


图 19-85 “选择服务器”对话框



图 19-86 “网络侦听器 IP 地址”对话框

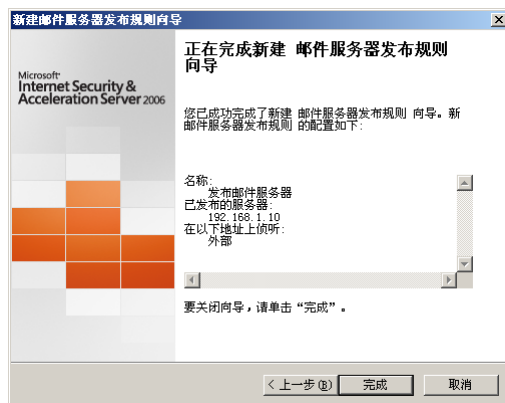


图 19-87 “正在完成新建邮件服务器发布规则向导”对话框

⑦ 单击“完成”按钮，发布完成邮件服务器。

这样，邮件服务器就可以通过 ISA Server 与 Internet 上的其他邮件服务器互相收发邮件，Internet 上的用户也可以使用 Foxmail 或 Outlook 等客户端程序收发邮件。需要注意的是，如果邮件服务器还支持以 Web 方式收发邮件，那么网络管理员还需要创建一条到该服务器的 Web 服务器发布规则。

19.5.3 发布 Exchange Web 客户端访问

如果邮件服务器使用 Exchange 2000、Exchange Server 2003 或 Exchange Server 2007 搭建，那么除了发布邮件服务器以外，还要发布 Exchange 的 Web 客户端访问。

① 在 ISA Server 2006 控制台中右击“防火墙策略”选项，从快捷菜单中选择“新建”→“Exchange Web 客户端访问发布规则”选项，打开“新建 Exchange 发布规则向导”对话框。

② 单击“下一步”按钮，显示如图 19-88 的“选择服务”对话框。在“Exchange 版本”下拉列表框中选择 Exchange 版本，在“Web 客户端邮件服务”选项组中选择“Outlook Web Access”复选框。

③ 单击“下一步”按钮，显示如图 19-89 所示的“发布类型”对话框，选择“发布单个网站或负载平衡器”单选按钮。

④ 单击“下一步”按钮，显示如图 19-90 所示的“服务器连接安全”对话框，这里选择“使用不安全的连接，连接发布的 Web 服务器或服务场”单选按钮。

⑤ 单击“下一步”按钮，显示如图 19-91 所示的“内部发布详细信息”对话框。在“内部站点名称”文本框中键入内部 Email 站点的名称，例如 mail.coolpen.net。选中“使用计算机名称或 IP 地址连接到发布的服务器”复选框，在“计算机名称或 IP 地址”文本框中输入邮件服务器的计算机名称或 IP 地址。

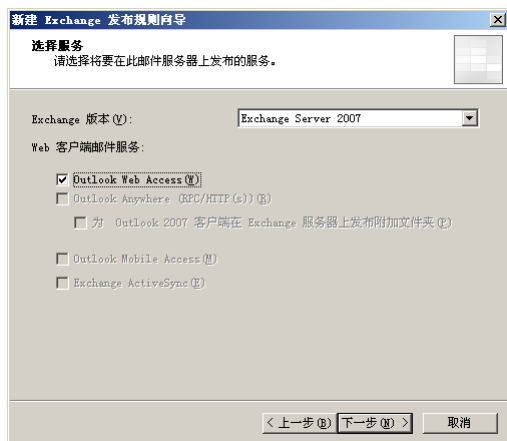


图 19-88 “选择服务”对话框

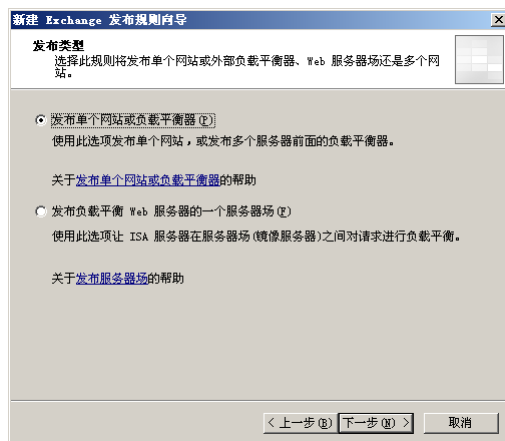


图 19-89 “发布类型”对话框

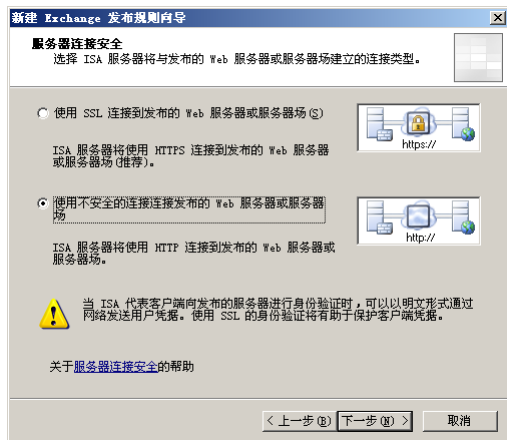


图 19-90 “服务器连接安全”对话框

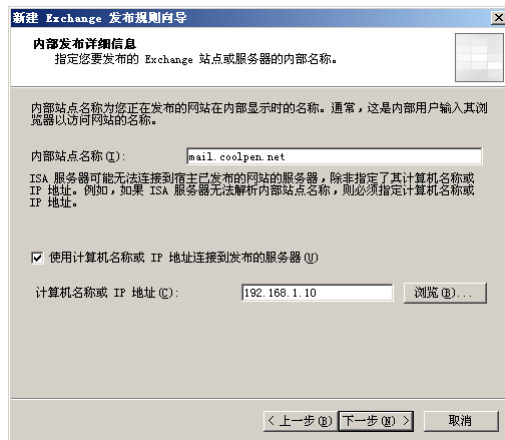


图 19-91 “内部发布详细信息”对话框

⑥ 单击“下一步”按钮，显示如图 19-92 所示的“公共名称细节”对话框。在“接受请求”下拉列表框中选择“此域名（在以下键入）”选项，在“公共名称”文本框中键入邮件服务器的域名，例如 mail.coolpen.net。



图 19-92 “公共名称细节”对话框

⑦ 单击“下一步”按钮，显示“选择 Web 侦听器”对话框，在“Web 侦听器”下拉列表框中选择前面创建的 Web 侦听器。

⑧ 单击“下一步”按钮，显示“身份验证委派”对话框，在下拉列表框中选择“无委派，客户

端无法直接进行身份验证”选项。

⑨ 单击“下一步”按钮，直到规则创建完成。然后单击“应用”按钮，使设置生效即可。

19.5.4 发布 SharePoint 站点

在 ISA Server 2006 中新增了一个“SharePoint 站点发布规则”功能，专门用来发布 SharePoint 站点。

① 在 ISA Server 2006 控制台，右击“防火墙策略”选项并选择快捷菜单中的“新建”→“SharePoint 站点发布规则”选项，打开“新建 SharePoint 发布规则向导”对话框。

② 单击“下一步”按钮，显示如图 19-93 所示的“发布类型”对话框，选择“发布单个网站或负载均衡器”单选按钮。

③ 单击“下一步”按钮，显示“服务器连接安全”对话框。如果 SharePoint 没有使用 SSL 安全连接，则选择“使用不安全的连接发布的 Web 服务器或服务场”单选按钮。

④ 单击“下一步”按钮，显示如图 19-94 所示的“内部发布详细信息”对话框。在“内部站点内容”文本框中输入 SharePoint 站点的名称，选中“使用计算机名称或 IP 地址连接到发布的服务器”复选框，并在“计算机名称或 IP 地址”文本框中输入 SharePoint 站点的 IP 地址。

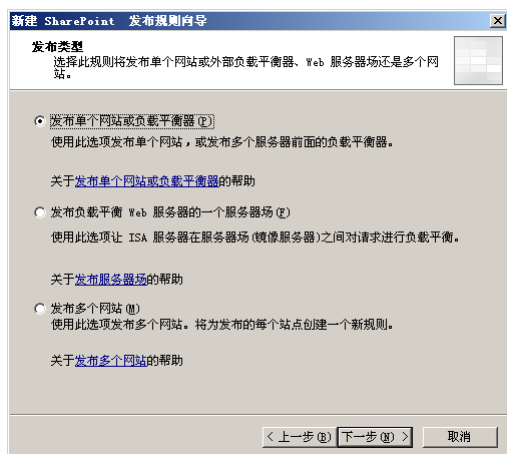


图 19-93 “选择发布类型”对话框

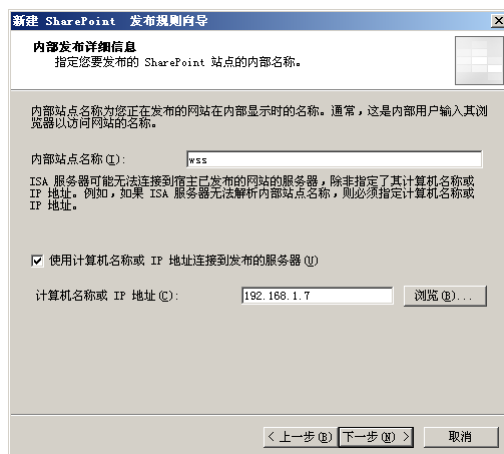


图 19-94 “内部发布详细信息”对话框

⑤ 单击“下一步”按钮，显示如图 19-95 所示的“公共名称细节”对话框。在“接受请求”下拉列表框中选择“此域名 (在以下输入)”选项，在“公共名称”文本框中输入 SharePoint 站点的 Internet 域名。

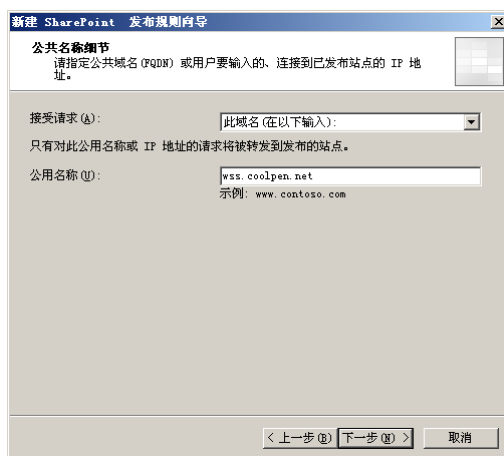


图 19-95 “公共名称细节”对话框

- ⑥ 在“选择 Web 侦听器”对话框中的“Web 侦听器”下拉列表框中选择已创建的 Web 侦听器。
- ⑦ 在“身份验证委派”对话框中选择“无委派，客户端无法直接进行身份验证”选项。
- ⑧ 在如图 19-96 所示的“备用访问映射配置”对话框中选择是否在 SharePoint 站点配置了 SharePoint AAM。

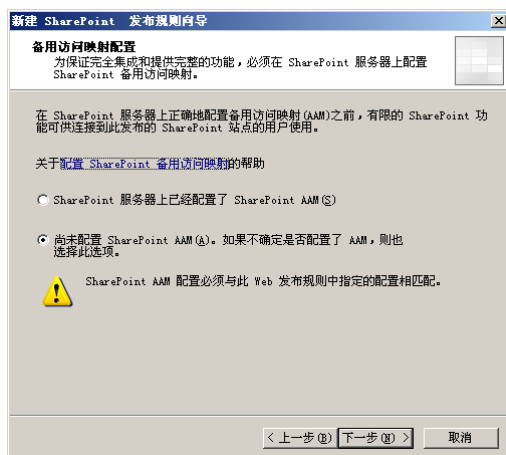


图 19-96 “备用访问映射配置”对话框

- ⑨ 单击“下一步”按钮，直到“新建 SharePoint 发布规则向导”完成，单击“应用”按钮使设置生效。

19.5.5 发布其他服务器

如果要在 ISA Server 2006 中发布其他服务器，如 FTP 服务器及终端服务器等，可以使用“非 Web 服务器协议发布规则”功能来实现。

- ① 以发布 FTP 服务器为例。在 ISA Server 2006 控制台中右击“防火墙策略”选项并从快捷菜单中选择“新建”→“非 Web 服务器协议发布规则”选项，打开“新建服务器发布规则向导”对话框。

- ② 当显示如图 19-97 所示的“选择服务器”对话框时，在“服务器 IP 地址”文本框中键入 FTP 服务器的 IP 地址。

- ③ 单击“下一步”按钮，显示如图 19-98 所示的“选择协议”对话框。在“选择的协议”下拉列表框中选择“FTP 服务器”选项。如果要发布其他服务器，则可选择相应的协议。



图 19-97 “选择服务器”对话框

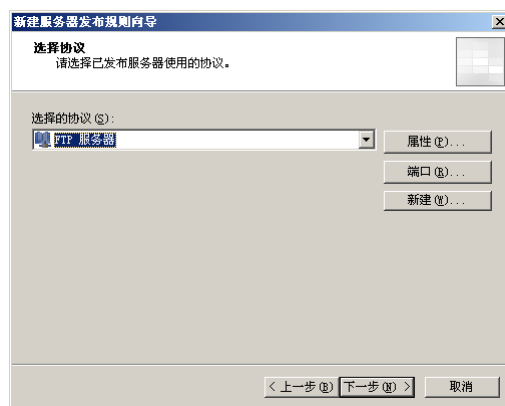


图 19-98 “选择协议”对话框



提示

如果在列表框中没有要发布的服务，则单击“新建”按钮创建，与添加 QQ 协议的过程类似。所不同的是，所有的服务都是“入站”协议，而访问规则都是“出站”协议。

④ 单击“端口”按钮，显示如图 19-99 所示的“端口”对话框，在其中设置防火墙端口和服务端端口。如果修改了默认端口，那么在访问时就必须加上相应的端口。

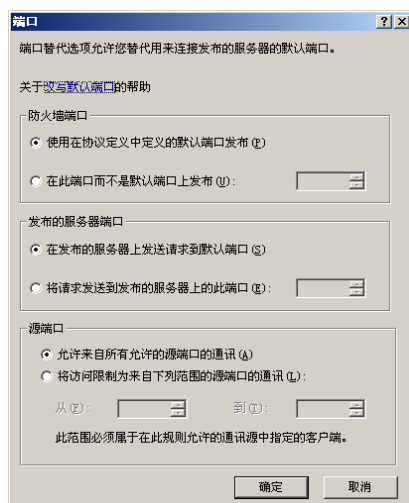


图 19-99 “端口”对话框

⑤ 在“网络侦听器 IP 地址”对话框中选中“外部”复选框。

⑥ 继续单击“下一步”按钮，直至创建完成规则，然后单击“应用”按钮使设置生效即可。

19.5.6 发布安全 Web 服务器

安全 Web 站点使用 https://方式访问，并且默认使用 TCP 的 443 端口。在同一台 Web 服务器中可以有多个使用 TCP 的 80 端口的普通 Web 站点，但只能有一个使用 TCP 的 443 端口的安全 Web 站点。如果要在同一台 Web 服务器中提供多个安全 Web 站点，只能使用 TCP 的 443 之外的其他端口。

发布安全的 Web 站点和发布 FTP 服务器一样，在“选择协议”对话框中选择“HTTPS 服务器”选项即可，如图 19-100 所示。



图 19-100 选择“HTTPS 服务器”选项

需要注意的是，在 ISA Server 2006 中，如果在同一个 Web 站点中既提供普通 Web 站点转发，又提供安全的 Web 站点转发，那么只能转发安全的 Web 站点，而不能提供普通的 Web 站点转发。

19.5.7 为 Internet 用户提供代理服务

如今，有很多用户使用 Internet 中的代理服务器上上网。这样对方显示的就是代理服务器的 IP 地址，而不是用户的真实地址，例如 IE 浏览器及 QQ 等软件。通常情况下，代理服务器需要有两个独立的与 Internet 的连接。而在 ISA Server 2006 中，只需有一个“Internet 出口”即可为 Internet 上的其他用户作

为代理服务器。

① 在 ISA Server 的管理控制台中，右击“防火墙策略”选项并选择快捷菜单中的“新建”→“非 Web 服务器协议发布规则”选项，打开“新建服务器发布规则向导”对话框。

② 在“选择服务器”对话框中的“服务器 IP 地址”文本框键入 ISA Server “内部网卡”的 IP 地址。

③ 在“选择协议”对话框中单击“新建”按钮，显示如图 19-101 所示的“新建协议定义向导”对话框，在“协议定义名称”文本框中键入一个名称。

④ 单击“下一步”按钮，显示“首要连接信息”对话框。单击“新建”按钮，显示如图 19-102 所示的“新建/编辑协议连接”对话框。在“协议类型”下拉列表框中选择“TCP”，在“方向”下拉列表框中选择“入站”选项，在“端口范围”中输入“8080”，单击“确定”按钮。

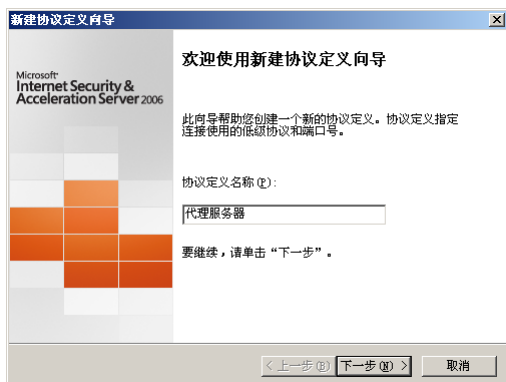


图 19-101 “新建协议定义向导”对话框

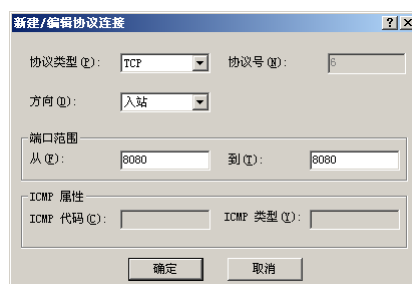


图 19-102 “新建/编辑协议连接”对话框

⑤ 在“辅助连接”对话框中选择“否”单选按钮，单击“下一步”按钮，直至“新建协议定义向导”完成。

⑥ 返回如图 19-103 所示的“选择协议”对话框，从“选择的协议”下拉列表框中选择新建的代理服务器协议。如果要更改防火墙端口，则单击“端口”按钮。

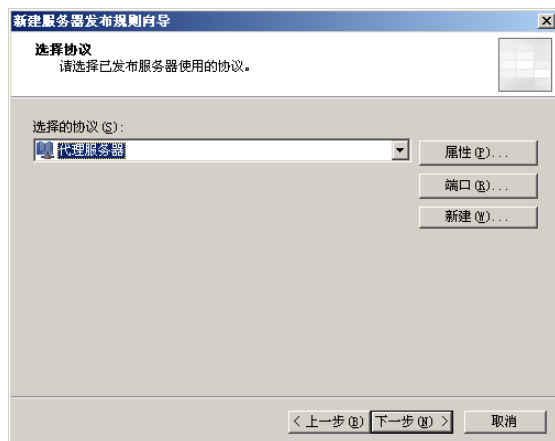


图 19-103 “选择协议”对话框

⑦ 在“网络侦听器 IP 地址”对话框中选中“外部”复选框，单击“下一步”按钮，直至服务器发布规则完成。

⑧ 在 ISA Server 2006 控制台中依次展开“配置”→“网络”选项。显示的“网络”窗口如图 19-104 所示。

⑨ 选择“内部”选项，右击并选择快捷菜单中的“属性”选项，显示如图 19-105 所示的“内部属性”对话框。

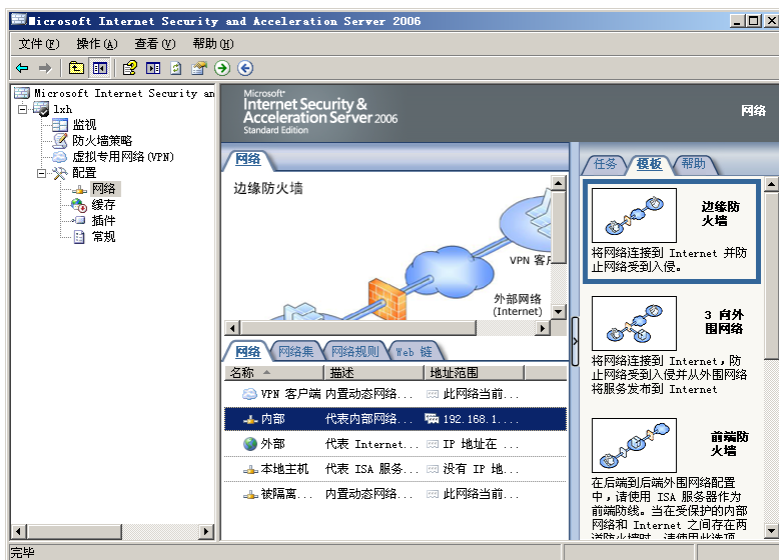


图 19-104 “网络”窗口

⑩ 打开如图 19-106 所示的“Web 代理”选项卡，选中“启用 Web 代理客户端”和“启用 HTTP”复选框，在“HTTP 端口”文本框中可以定义端口号。



图 19-105 “内部 属性”对话框

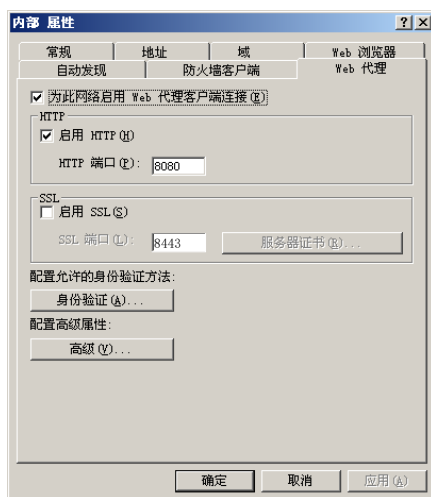


图 19-106 “Web 代理”选项卡

⑪ 单击“确定”按钮保存，并返回 ISA Server 2006 控制台，单击“应用”按钮使设置生效。至此，代理设置完成，在客户端上即可使用该代理。以 IE 浏览器为例。操作步骤如下。

① 打开 IE 浏览器，选择“工具”→“Internet 选项”选项。在“连接”选项卡中单击“局域网设置”按钮，显示“局域网 (LAN) 设置”对话框。

② 选中“为 LAN 使用代理服务器”复选框，在“地址”和“端口”文本框中键入 ISA 服务器的外网地址及代理服务协议端口。然后选中“跳过本地地址的代理服务器”复选框，如图 19-107 所示。

③ 单击“确定”保存即可，在其他软件中也可以使用该代理。

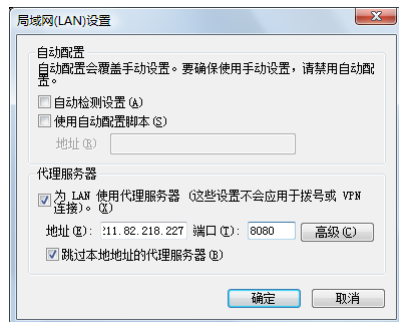


图 19-107 设置代理服务器

19.6 实现安全 VPN 访问服务

如果将 ISA Server 配置成 VPN 服务器，可以将分布在各地的分公司或办事处组成虚拟局域网。在通常情况下 VPN 服务器与其他服务不能“共存”于同一台服务器上，因为在启用 VPN 服务之后系统默认的路由表发生了改变，不能使用其他网络通信。而有了 ISA Server 2006，这一切就变得非常简单了。

19.6.1 在 ISA Server 中启用 VPN 服务器

要在 ISA Server 服务器上启用 VPN 服务器，必须首先在“路由和远程访问”中停止“路由和远程访问”服务，然后在 ISA Server 中启用 VPN 并创建访问规则。

① 单击“开始”→“管理工具”→“路由和远程访问”选项，禁用路由和远程访问服务，如图 19-108 所示。

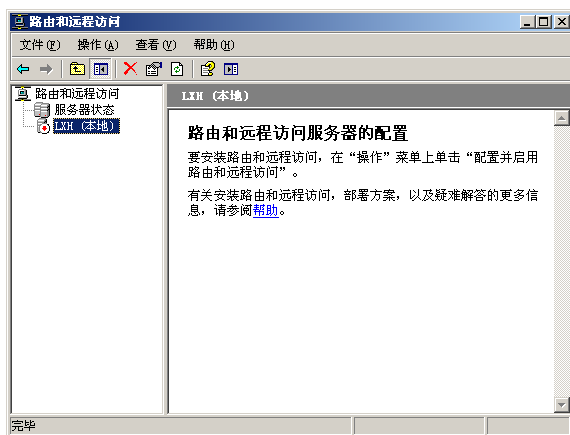


图 19-108 禁用路由和远程访问服务

② 打开 ISA Server 2006 控制台，在左窗格中选择“虚拟专用网络 (VPN)”选项，显示的“虚拟专用网络 (VPN)”窗口如图 19-109 所示。



图 19-109 “虚拟专用网络 (VPN)”窗口

③ 在右侧的“VPN 客户端任务”选项区域中单击“配置 VPN 客户端访问”链接，显示如图 19-110 所示的“VPN 客户端属性”对话框。在“常规”选项卡中，清除“启用 VPN 客户端访问”复选框。

④ 打开如图 19-111 所示的“协议”选项卡，选择远程连接要使用的隧道协议，默认为“PPTP”。如果使用 L2TP，还需要在客户端和服务端配置证书。

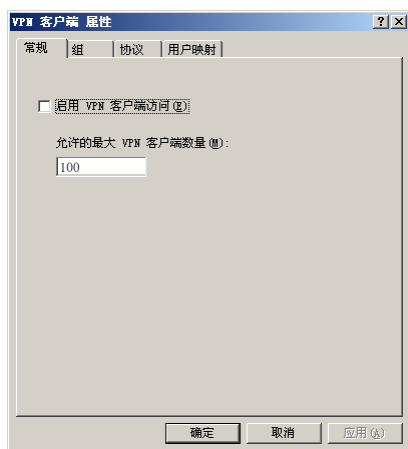


图 19-110 “VPN 客户端属性”对话框

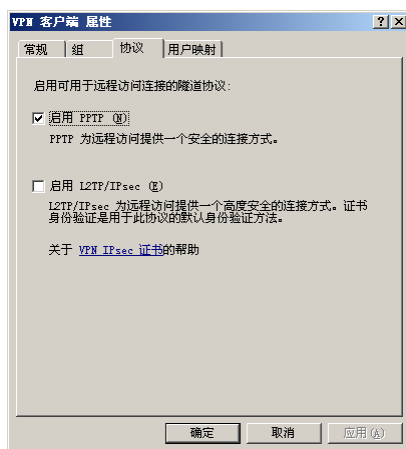


图 19-111 “协议”选项卡

⑤ 单击“确定”按钮，返回 ISA Server 2006 控制台。在“虚拟专用网络 (VPN)”窗口右侧的“常规 VPN 配置”栏中单击“选择访问网络”超级链接，显示“虚拟专用网络 (VPN) 属性”对话框，在如图 19-112 所示的“访问网络”选项卡中选择客户端初始化时连接到的 VPN 服务器的网络。如果只作为 VPN 服务器对外提供 VPN 接入服务，则默认选择“外部”复选框；对于站点到站点的连接，选择“内部”复选框。

⑥ 打开如图 19-113 所示的“地址分配”选项卡，设置为 VPN 客户端分配 IP 地址的方式。如果为客户端分配静态 IP 地址，选择“静态地址池”单选按钮，单击“添加”按钮添加 IP 地址段；如果网络中存在 DHCP 服务器，则选择“动态主机配置协议 (DHCP)”单选按钮，为客户端分配动态 IP 地址。

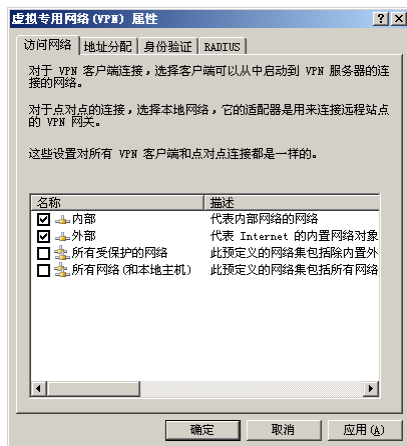


图 19-112 “访问网络”选项卡

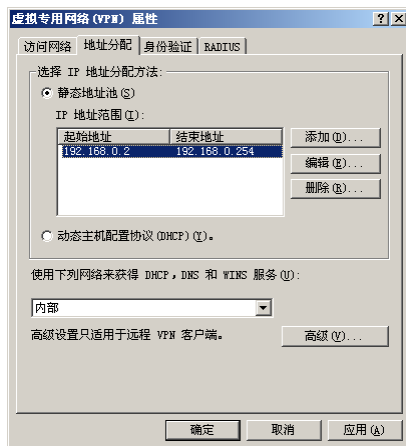


图 19-113 “地址分配”选项卡

注意：

如果配置静态地址，则必须定义一个与本地主机内部网卡不相关的地址段。即地址范围不能与本地主机、外网的子网重复，也不能与路由表中已有的地址冲突。

⑦ 单击“确定”按钮，返回 ISA Server 2006 控制台。在“虚拟专用网络 (VPN)”窗口右侧的

“VPN 客户端任务”栏中单击“启用 VPN 客户端访问”超级链接。

⑧ 右击“防火墙策略”选项，选择快捷菜单中的“新建”→“访问规则”选项，创建一条规则。在“规则操作”对话框中选择“允许”单选按钮，在“协议”对话框中选择“所有出站通信”，在“访问规则源”对话框中添加“VPN 客户端”，在“访问规则目标”对话框中根据需要选择内部、本地主机或者外部。

⑨ 创建完成规则以后，单击“应用”按钮使设置生效，并重新启动计算机。

19.6.2 检查与配置 VPN 服务器

配置完成 ISA Server 2006 中的 VPN 服务以后，打开“路由和远程访问”控制台。如果“路由和远程访问”已经自动启动（如图 19-114 所示），则表示 ISA Server 2006 中的 VPN 服务器配置完成；否则需要启用并配置“路由和远程访问”，启用“VPN 访问”功能。具体操作步骤请参见相关内容，这里不再赘述。

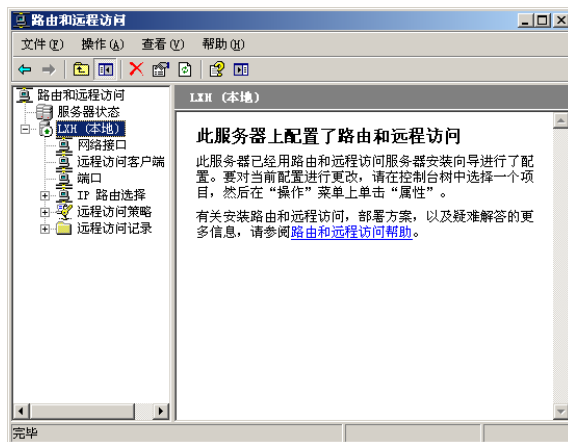


图 19-114 路由和远程访问

19.6.3 管理与设置用户

VPN 服务器配置完成以后，可以为 VPN 用户启动 VPN 拨入功能。打开 VPN 用户的属性对话框，在“拨入”选项卡中选择“允许访问”单选按钮，远程 VPN 客户端可以使用此用户名拨入 VPN 服务器。如果没有启用 DHCP 服务器，则可选中“分配静态 IP 地址”复选框，为用户指定静态 IP 地址，如图 19-115 所示。

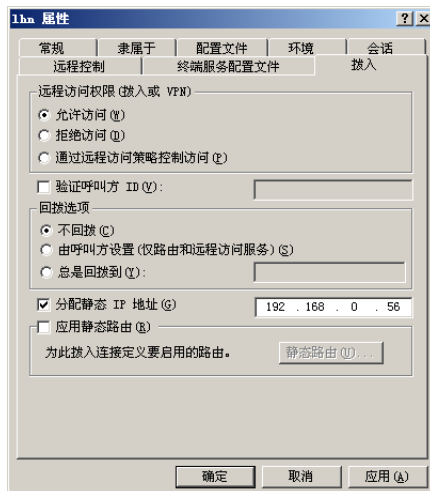


图 19-115 为用户启用 VPN 功能

19.7 高效访问 Internet

ISA Server 具有缓存功能, 可以将客户端经常访问的内容作为缓存保存在磁盘中。当用户请求访问 Web 对象时即可直接从本地缓存中查询内容并返回给客户端, 而不必通过 Internet。由于直接在磁盘缓存中调用文件, 所以相比 Internet 不仅大大减少了响应时间, 提高了处理速度, 而且减少了 Internet 带宽的占用。

19.7.1 启用缓存

缓存实际上是磁盘上用来保存 Web 内容的一部分空间, 在 ISA Server 2006 中可以在多个分区中创建缓存。但为了系统安全起见, 建议不要将缓存分配到系统分区中。

① 在 ISA Server 2006 控制台中依次展开“配置”→“缓存”选项, 显示如图 19-116 所示的“缓存驱动器”窗口。

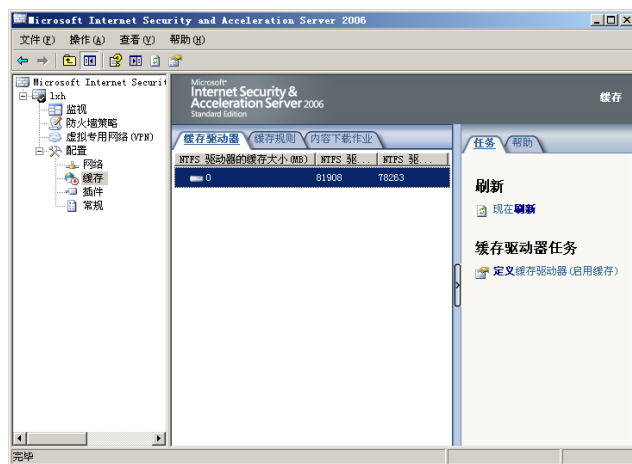


图 19-116 “缓存驱动器”窗口

② 在右窗格的“任务”选项卡中单击“定义缓存驱动器（启用缓存）”超级链接, 显示如图 19-117 所示的“定义缓存驱动器”对话框。选择一个非系统分区, 并在“最大缓存大小”文本框中输入待分配给缓存容量大小, 单击“设置”按钮即可设置缓存。如果有多个可用的 NTFS 分区, 可以在其中均创建缓存。

③ 单击“确定”按钮保存, 在 ISA Server 2006 控制台中单击“应用”按钮, 显示如图 19-118 所示的“ISA 服务警告”对话框, 选择“保存更改, 并重启动服务”单选按钮。



图 19-117 “定义缓存驱动器”对话框



图 19-118 “ISA 服务警告”对话框

- ④ 单击“确定”按钮，重新启动服务即可。

19.7.2 创建正向缓存

ISA Server 支持正向缓存，即从内部到外部网络（即 Internet 网络）访问的缓存，可以使客户端更快地访问所请求的内容。当客户端向服务器请求 Web 对象时，ISA 服务器会检查该对象是否存在于缓存中。如果存在，则直接返回给客户端；否则会从 Internet 中的服务器请求，将对象返回给客户端。同时在 ISA 服务器上将对对象的一个副本保留在缓存中，以便下次响应客户端的请求。

- ① 在 ISA Server 2006 控制台中打开“缓存”窗口中的“缓存规则”选项卡，如图 19-119 所示。

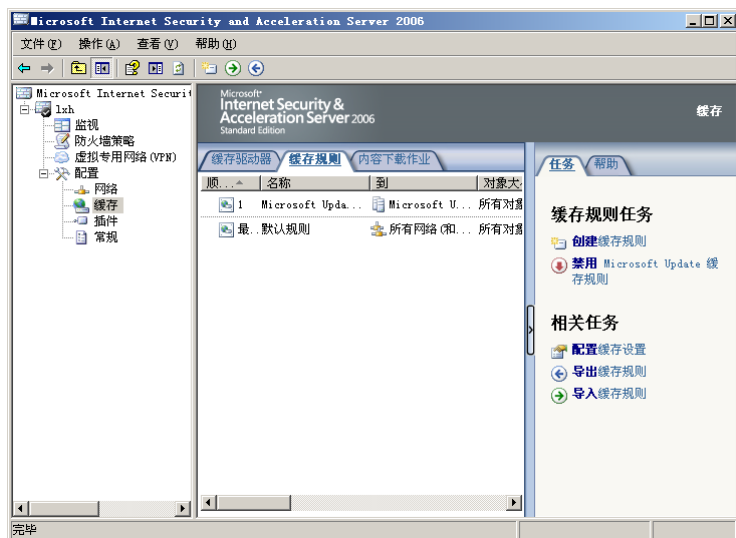


图 19-119 “缓存规则”选项卡

- ② 在右窗格的“缓存规则任务”栏中单击“创建缓存规则”选项，打开“新缓存规则向导”对话框，如图 19-120 所示。为缓存规则键入一个名称，例如“正向缓存”。

- ③ 单击“下一步”按钮，显示如图 19-121 所示的“缓存规则目标”对话框。单击“添加”按钮，从“网络实体”中添加“外部”网络。

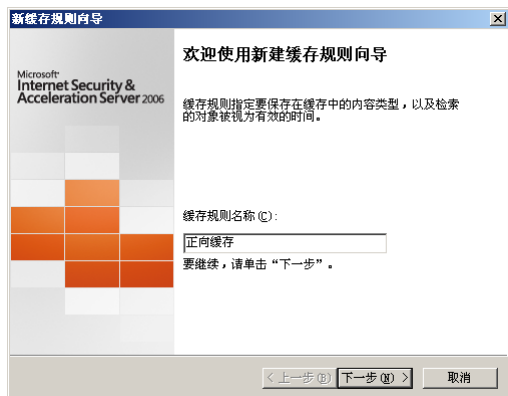


图 19-120 “新缓存规则向导”对话框

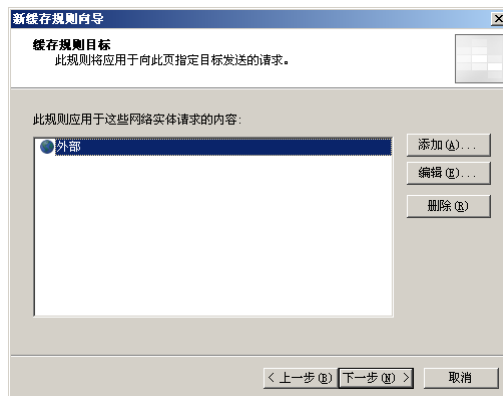


图 19-121 “缓存规则目标”对话框

- ④ 单击“下一步”按钮，显示如图 19-122 所示的“内容检索”对话框，选择“只有在缓存中存在对象的一个有效版本……”单选按钮。

- ⑤ 单击“下一步”按钮，显示如图 19-123 所示的“缓存内容”对话框，选择“如果源和请示头指明要缓存”单选按钮。

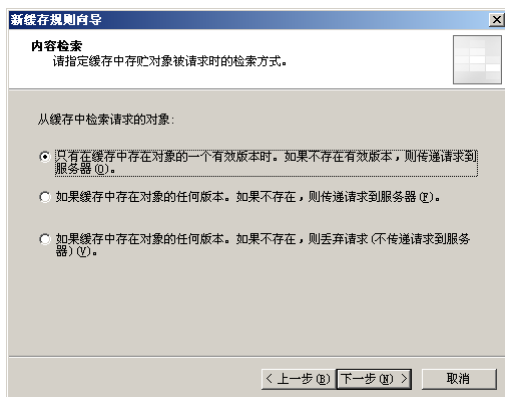


图 19-122 “内容检索”对话框

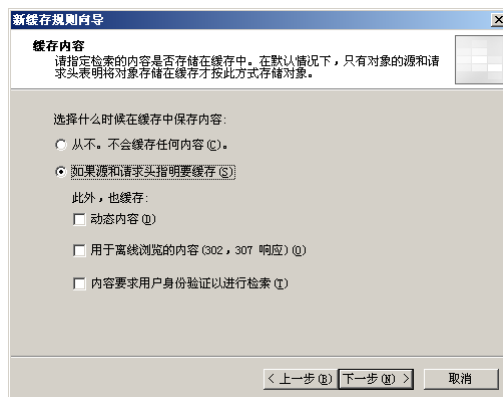


图 19-123 “缓存内容”对话框

⑥ 单击“下一步”按钮，显示如图 19-124 所示的“缓存高级配置”对话框。选中“不缓存大于此大小的对象”复选框，并设置对象的大小，例如 1 MB。当对象大小超过 1 MB 时，将不进行缓存。

⑦ 单击“下一步”按钮，显示如图 19-125 所示的“HTTP 缓存”对话框，选择“启用 HTTP 缓存”复选框。

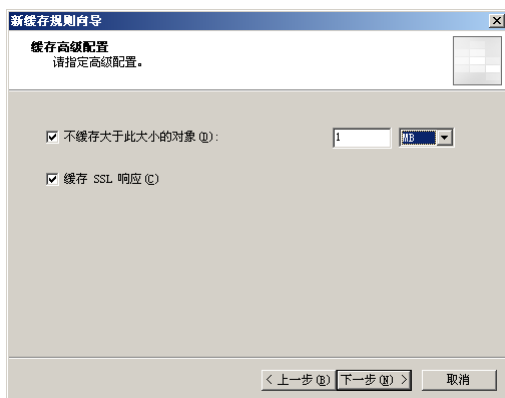


图 19-124 “缓存高级配置”对话框

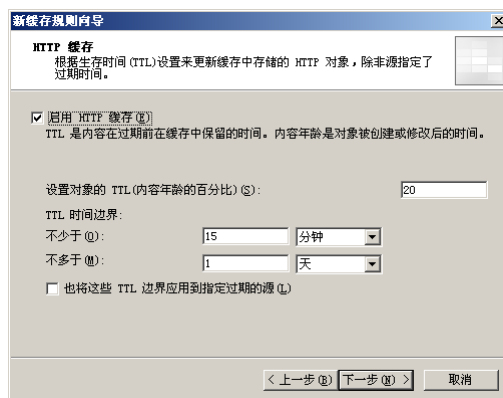


图 19-125 “HTTP 缓存”对话框

⑧ 单击“下一步”按钮，显示如图 19-126 所示的“FTP 缓存”对话框。选中“启用 FTP 缓存”复选框，并根据实际情况选择 FTP 缓存时间。

⑨ 单击“下一步”按钮，显示如图 19-127 所示的“正在完成新建缓存规则向导”对话框。

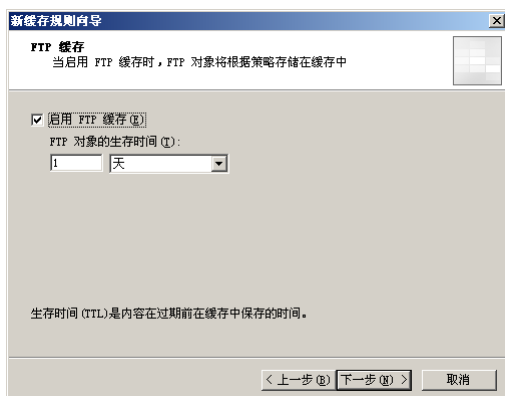


图 19-126 “FTP 缓存”对话框

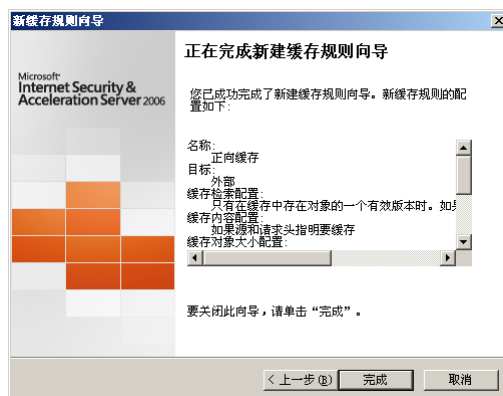


图 19-127 “正在完成新建缓存规则向导”对话框

⑩ 单击“完成”按钮，创建完成缓存规则，然后单击“应用”按钮使设置生效。

19.7.3 禁止反向缓存

反向缓存是指 Internet 的用户访问经过 ISA Server 发布的服务器时，由 ISA Server 服务器代替 Internet 的用户访问并缓存访问内容。不过，如果 ISA Server 发布的 Web 站点经常被更新，通常需要禁用反向缓存；否则用户访问的缓存将是以前站点的内容。

① 在 ISA Server 2006 控制台的“缓存”窗口中单击“创建缓存规则”链接，打开如图 19-128 所示的“新缓存规则向导”对话框，为该规则键入一个名称。

② 单击“下一步”按钮，显示“缓存规则目标”对话框。单击“添加”按钮，显示“添加网络实体”对话框，单击“新建”菜单中的“子网”选项，显示如图 19-129 所示的“新建子集规则元素”对话框，创建一个子网。单击“确定”按钮，将子网添加到“缓存规则目标”中。

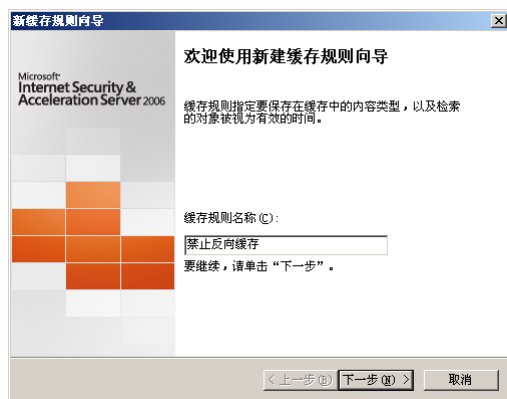


图 19-128 “新缓存规则向导”对话框

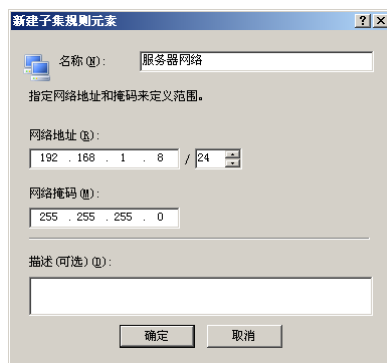


图 19-129 “新建子集规则元素”对话框

③ 单击“下一步”按钮，显示“内容检索”对话框，使用默认值即可。

④ 单击“下一步”按钮，显示如图 19-130 所示的“缓存内容”对话框，选择“从不。不会缓存任何内容(C)”单选按钮。

⑤ 单击“下一步”按钮，直到规则创建完成。返回“缓存规则”窗口，选择新建的“禁止反向缓存”规则。右击并从快捷菜单中选择“属性”选项，显示“禁止反向缓存 属性”对话框。打开如图 19-131 所示的“HTTP”选项卡，清除“启用 HTTP 缓存”复选框。

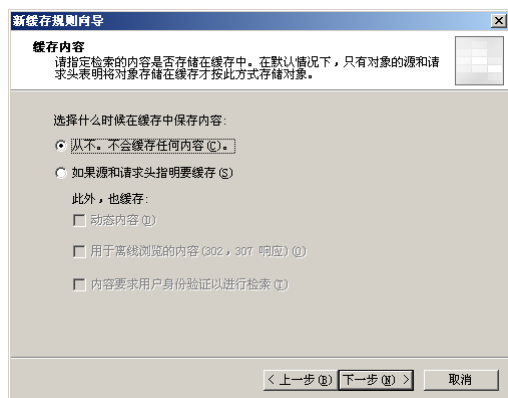


图 19-130 “缓存内容”对话框

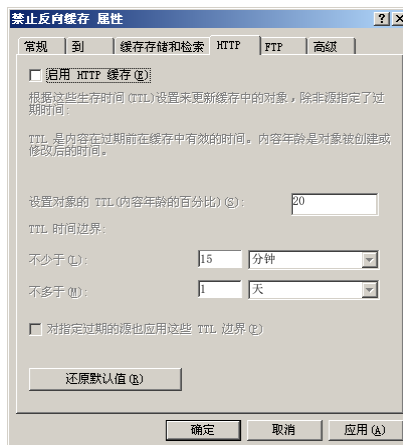


图 19-131 “HTTP”选项卡

⑥ 打开如图 19-132 所示的“FTP”选项卡，清除“启用 FTP 缓存”复选框。

⑦ 单击“确定”按钮，并在 ISA Server 2006 控制台中单击“应用”按钮使设置生效。

19.7.4 禁止缓存某些站点

在 ISA Server 中，可以禁止缓存某些特定站点。例如，禁止缓存邮件服务器，避免访问过期的或错误的内容等。

① 选择所创建的“正向缓存”规则，右击并从快捷菜单中选择“属性”选项，打开“允许正向缓存 属性”对话框。打开“到”选项卡，如图 19-133 所示。

② 在“例外”选项组中单击“添加”按钮，显示“添加网络实体”对话框。单击“新建”菜单中的“URL 集”选项，打开“新建 URL 集规则元素”对话框。在“名称”文本框中键入一个名称，单击“添加”按钮添加常用的邮件服务器的 URL 地址，如图 19-134 所示。

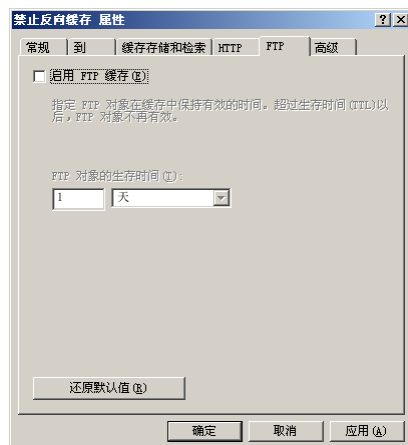


图 19-132 “FTP”选项卡

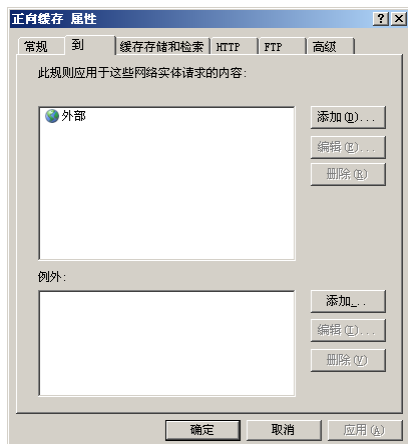


图 19-133 “到”选项卡



图 19-134 添加邮件服务器地址

③ 单击“确定”按钮保存，并将其添加到“例外”列表框中，如图 19-135 所示。



图 19-135 添加邮件列表

④ 单击“确定”按钮保存设置，然后在 ISA Server 2006 控制台中将该规则移动到上面，并单击“应用”按钮使规则生效。

19.8 备份与恢复 ISA Server 2006

ISA Server 2006 主要通过规则控制网络，因此会创建多个规则。如果 ISA 服务器出现故障、迁移

或者重新安装 ISA Server 2006，在重新配置时将非常麻烦。为了防止因服务器故障而造成数据丢失，或者要迁移或重新安装 ISA Server 2006，可事先备份 ISA Server 中的配置，以便日后恢复。

19.8.1 备份防火墙策略

备份 ISA Server 2006 的防火墙策略可利用“导出向导”来完成，导出的配置将保存为 xml 文件。为了安全起见，建议将已备份的策略保存在网络磁盘中，以免误删或者丢失。

① 在 ISA Server 2006 控制台中右击“防火墙策略”选项，选择快捷菜单中的“导出”选项，打开“导出向导”对话框，如图 19-136 所示。

② 单击“下一步”按钮，显示如图 19-137 所示的“导出首选项”对话框。如果要加密导出的用户密码、RADIUS 共享信息，以及其他安全信息，则选中“导出机密信息”复选框，并在“密码”文本框中设置一个至少 8 个字符的密码。



图 19-136 “导出向导”对话框

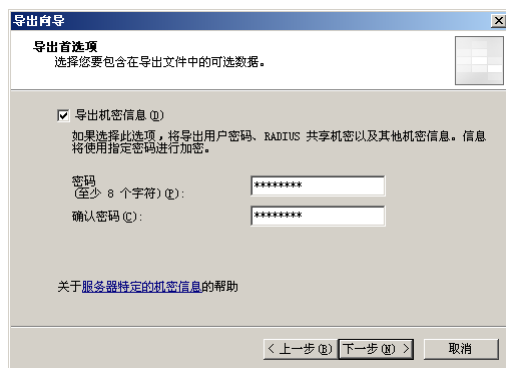


图 19-137 “导出首选项”对话框

③ 单击“下一步”按钮，显示如图 19-138 所示的“导出文件位置”对话框。单击“浏览”按钮，选择导出的配置文件的保存路径，并设置一个文件名。

④ 单击“下一步”按钮，显示如图 19-139 所示的“正在完成导出向导”对话框，提示导出向导已完成。

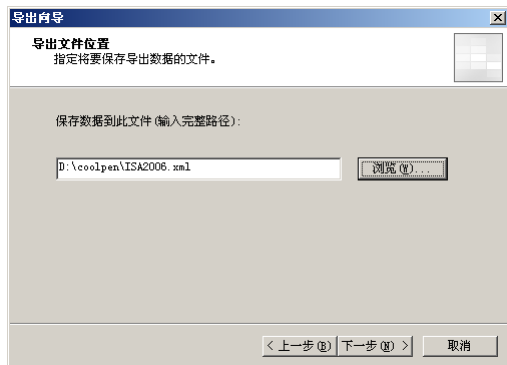


图 19-138 “导出文件位置”对话框



图 19-139 “正在完成导出向导”对话框

⑤ 单击“完成”按钮，开始导出防火墙策略，如图 19-140 所示。

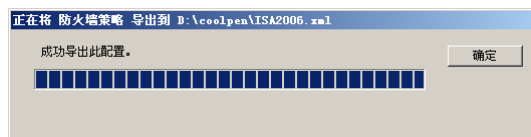


图 19-140 导出防火墙策略

⑥ 单击“确定”按钮，防火墙策略备份完成。

如果要导出“防火墙策略”中的某个对象，例如只备份某个协议，则选择要备份的对象。右击并选择快捷菜单中的“导出选择的”选项，即可启动“导出向导”将其导出。

19.8.2 备份 ISA Server 2006 的所有配置

ISA Server 2006 中的配置非常多，“防火墙策略”只是其中的一部分。如果要导出 ISA Server 2006 的所有配置，则利用“导出向导”来完成。

① 在 ISA Server 2006 控制台中选择计算机名，右击并选择快捷菜单中的“导出（备份）”选项，打开“导出向导”对话框。

② 单击“下一步”按钮，显示如图 19-141 所示的“导出首选项”对话框。建议选中“导出机密信息”复选框，设置一个键入密码。如果同时要导出委派给用户和组和管理角色，则选中“导出用户权限设置”复选框。

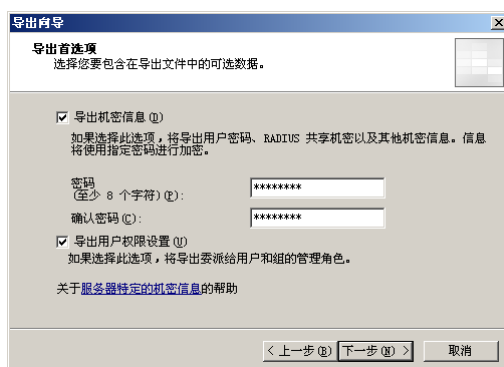


图 19-141 “导出首选项”对话框

③ 单击“下一步”按钮，显示“导出文件位置”对话框。键入配置文件的保存位置及文件名，然后继续单击“下一步”按钮，直至导出完成。

19.8.3 恢复 ISA Server 2006 的配置

当重新安装 ISA Server 2006，或者迁移到新服务器上以后，就可以利用原来的备份文件恢复，而不必重新创建规则。恢复 ISA 服务器的所有配置和恢复防火墙策略的过程完全相同，只是需要选择相应的备份文件。

① 选择要恢复配置的项目，例如“防火墙策略”或者服务器名。右击并选择快捷菜单中的“导入”选项，打开如图 19-142 所示的“导入向导”对话框。

② 单击“下一步”按钮，显示如图 19-143 所示的“选择导入文件”对话框。单击“浏览”按钮，选择已备份的文件。



图 19-142 “导入向导”对话框

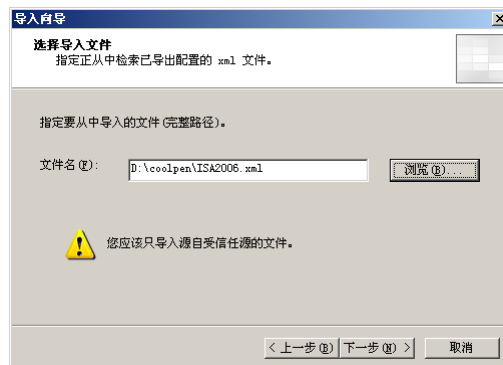


图 19-143 “选择导入文件”对话框

③ 单击“下一步”按钮，显示如图 19-144 所示的“导入首选项”对话框。如果要导入服务器特定信息，则选中“导入服务器特定信息”复选框。

④ 单击“下一步”按钮，显示如图 19-145 所示的“输入密码”对话框，在“密码”文本框中键入备份时设置的密码。

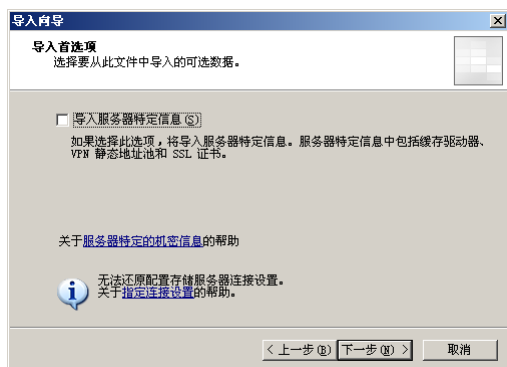


图 19-144 “导入首选项”对话框

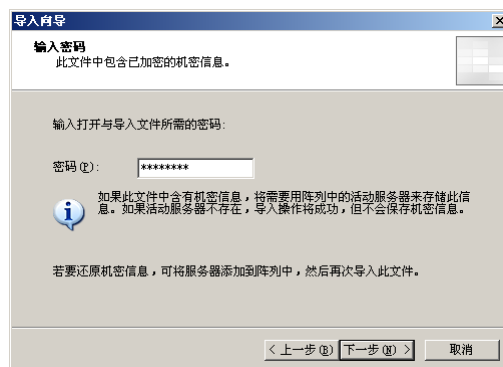


图 19-145 “输入密码”对话框

⑤ 单击“下一步”按钮，显示如图 19-146 所示的“正在完成导入向导”对话框，提示导入向导已完成。

⑥ 单击“完成”按钮，显示如图 19-147 所示的“成功导入配置”提示信息。单击“确定”按钮，恢复完成 ISA Server 服务器。

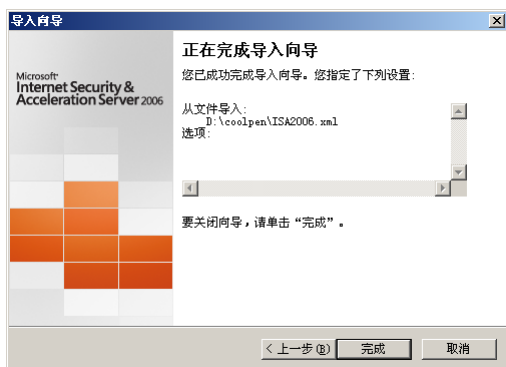


图 19-146 “正在完成导入向导”对话框



图 19-147 “成功导入配置”提示信息

第 20 章 配置与管理网络防病毒服务

病毒防御是网络安全管理工作的重中之重，个别客户端感染病毒后在极短的时间内就可能感染整个网络，从而造成网络服务中断或瘫痪。防范病毒最常用的方法就是在网络中部署专业杀毒软件，如 Symantec AntiVirus、趋势科技和瑞星等产品的企业版。在网络中配置专业防病毒服务器后，即可实现对所有客户端的实时安全管理，包括病毒扫描查杀、E-mail 实时检测及病毒库升级等。

20.1 安装 Symantec Endpoint Protection 企业版

Symantec Endpoint Protection 是 Symantec 公司近期推出的新一代企业版网络安全防护产品，它将 Symantec AntiVirus 与高级威胁防御功能相结合，可以为笔记本电脑、台式电脑和服务器提供无与伦比的恶意软件防护能力。Symantec Endpoint Protection 在一个代理和管理控制台中集成了基本安全技术，既节约成本，又可以提高网络安全防护能力。

20.1.1 Symantec 产品简介

新一代 Symantec 安全防护产品主要包括 Symantec Endpoint Protection（端点保护）和 Symantec Network Access Control（端点网络访问控制），每一种产品都可以提供功能强大的 Symantec Endpoint Protection Manager，以帮助管理员快速完成网络安全的统一部署和管理。

1. Symantec Endpoint Protection 的功能与特点

Symantec Endpoint Protection 可保护端点计算设备不受病毒威胁和风险侵袭，并为端点计算机提供 3 层防护，分别是网络威胁防护、主动型威胁防护，以及防病毒和防间谍软件防护，如图 20-1 所示。网络威胁防护通过使用规则和特征，可禁止威胁访问被保护计算机；主动型威胁防护可根据威胁的行为标识并降低威胁；防病毒和防间谍软件防护使用 Symantec 创建的特征，识别并削弱尝试访问或已访问被保护计算机的威胁。

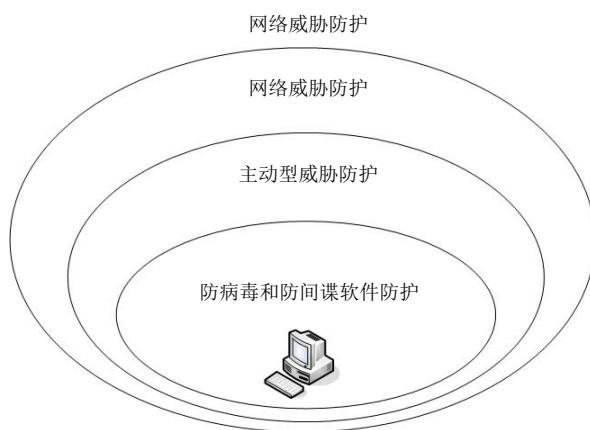


图 20-1 Symantec Endpoint Protection 的 3 层防护

(1) 网络威胁防护

网络威胁防护包括防火墙和入侵防护软件，可保护用户的端点计算设备。防火墙支持为特定端口和特定应用程序写入的规则，并检查所有网络通信使用状态。因此对于由客户端发起的所有网络通信，

只需要创建出站规则即可支持，状态检查会自动允许响应出站通信的返回通信。防火墙完全支持 TCP、UDP、ICMP 和所有 IP 协议（如 ICMP 和 RSVP），并支持以太网和令牌环协议。还可以禁止协议驱动程序，如 VMware 和 WinPcap。防火墙可自动识别合法的 DNS、DHCP 和 WINS 通信，因此可以允许此通信，而不写入规则。



注意：

默认状态下，Symantec 假设用户已创建防火墙规则，从而拒绝所有不允许的通信。
防火墙不支持 IPv6。



入侵防护引擎支持检查端口扫描和拒绝服务攻击，并可阻挡缓冲区溢出攻击支持自动禁止来自受感染计算机的恶意通信，入侵检测引擎支持深度数据包检查及正则表达式，并且允许用户创建使用类似 Snort 格式的自定义特征。

(2) 主动型威胁防护

主动型威胁防护可根据计算机上进程的行为识别威胁，例如，蠕虫、病毒、特洛伊木马，以及记录击键情况的程序，TruScan 主动型威胁扫描根据这些威胁的行为和特性（而不是根据传统的安全特征）来识别它们。主动型威胁扫描会针对数百种的检测模块分析威胁的行为，以确定活动的进程是安全，还是具有恶意的。此项技术可以在不使用传统的特征或补丁程序的情况下，通过威胁的行为立即检测和降低未知的威胁。

在 32 位操作系统中通过主动型威胁防护还可控制对硬件设备、文件和注册表键的读取、写入和执行访问。如有必要，用户可以改善对特定支持的操作系统的支持，也可以通过类 ID 禁用外围设备（例如 USB、蓝牙、红外线、FireWire、串口、并口、SCSI 和 PCMCIA）。

(3) 防病毒和防间谍软件威胁防护

防病毒和防间谍软件威胁防护通过扫描引导扇区、内存与文件检测其中是否有病毒、间谍软件和安全风险，防止计算机受感染。防病毒和防间谍软件威胁防护使用病毒和安全风险特征，可在病毒定义文件中找到这些特征。此防护通过在不影响计算机不稳定的情况下，在安全风险安装前首先予以禁止，也可保护计算机。

防病毒和防间谍威胁防护包括自动防护，可检测尝试访问内存或自行安装的病毒和安全风险。自动防护也会扫描安全风险，如广告软件和间谍软件。当其发现安全风险时会受感染文件隔离，或者消除和弥补安全风险的负面影响，也可以在自动防护中禁用安全风险扫描。自动防护可修复复杂的风险，例如隐藏用户模式风险（Rootkit），还可修复难以删除或者会重新自我安装的永久性安全风险。

防病毒和防间谍软件威胁防护也包括自动防护，监控所有 POP3 和 SMTP 通信扫描 Internet 电子邮件程序。用户可以配置防病毒和防间谍软件威胁防护，使其扫描传入消息是否有威胁和安全风险，以及扫描传出消息是否进行已知启发式扫描。扫描传出电子邮件有助于阻止威胁（如蠕虫）的传播，它们可以使用电子邮件客户端在网络中复制。



注意：

在服务器型操作系统中会禁止安装 Web 型 Internet 电子邮件程序的自动防护，例如，用户不能在 Windows Server 2003 上安装此功能。



2. Symantec Network Access Control 概述

Symantec Network Access Control 即网络访问控制，不允许未经授权、配置不当和受感染的端点计算设备访问网络，从而保护网络，类似于 Windows Server 2008 中的网络访问保护策略（NAP）。例如，Symantec Network Access Control 可拒绝未运行特定版本的软件和特征的客户端访问网络。如果客户端不符合要求，则 Symantec Network Access Control 可以隔离相应计算机并对其实施补救措施。如果客

户端中的病毒定义早于一周，则 Symantec Network Access Control 可以隔离计算机。它可使用最新的病毒定义更新计算机（补救），然后允许计算机访问网络。

Symantec Network Access Control 允许用户使用主机完整性策略来控制这项防护，用户可以使用 Symantec Endpoint Protection Manager 控制台创建主机完整性策略，然后将策略应用于客户端组。如果只安装了 Symantec Network Access Control 客户端软件，则用户可以要求客户端运行防病毒、防间谍软件和防火墙软件。此外还可以请求这些计算机运行最新的操作系统 Service Pack 和补丁程序，并创建自定义应用程序要求。如果客户端不符合策略，用户就可以更新它们。

如果将 Symantec Network Access Control 与 Symantec Endpoint Protection 集成，则可以将防火墙策略应用于不符合主机完整性策略的客户端。此策略会限制客户端可用于网络访问的端口，也可限制客户端可访问的 IP 地址。例如，可以限制非遵从计算机只与包含所需软件和更新的计算机通信，这种集成称为“自我强制执行”。

如果将 Symantec Network Access Control 与称为“Symantec Enforcer”的可选硬件设备集成，则可以进一步限制不遵从的计算机访问用户的网络。用户可以将这些不遵从的计算机限制在特定的网络区段以进行补救，也可以完全禁止这些计算机进行访问。例如，使用 Symantec Gateway Enforcer 时，可以控制外部计算机通过 VPN 访问网络。使用 Symantec DHCP 和 LAN Enforcer 可以通过将不可路由的 IP 地址分配给非遵从计算机控制内部计算机访问网络，也可以将非遵从计算机分配至隔离的 LAN 区段。

3. Symantec Endpoint Protection Manager 概述

Symantec Endpoint Protection Manager 包括两个基于 Web 的应用程序，其中一个基于 Web 的应用程序需要 Microsoft Internet 信息服务（IIS），必须首先安装 IIS 才能安装 Symantec Endpoint Protection Manager；另一个基于 Web 的应用程序运行在 Apache Tomcat 上，它是自动安装的。Symantec Endpoint Protection Manager 包括一个嵌入式数据库和 Symantec Endpoint Protection Manager 控制台。用户可以自动安装嵌入式数据库，也可以将数据库安装到 Microsoft SQL Server 2000/2005 实例中。

如果用户的网络属于小型网络，并且位于一个地理位置，那么只需要安装一个 Symantec Endpoint Protection Manager；如果用户的网络分散在不同地点，则可能需要安装额外的 Symantec Endpoint Protection Manager，以用于负载平衡和带宽分配；如果用户的网络非常庞大，则可以安装带有附加数据库的额外 Symantec Endpoint Protection Manager 站点，并将其配置为通过复制共享数据；如果要提供额外的冗余，可以安装额外的 Symantec Endpoint Protection Manager 站点以支持故障转移。

4. 可选组件

可与 Symantec Endpoint Protection Manager 搭配使用的组件如表 20-1 所示。

表 20-1 可与 Symantec Endpoint Protection Manager 搭配使用的组件

组 件	描 述
Symantec Endpoint Protection Manager 控制台	帮助网络管理员管理 SEP 服务器和客户端，如更新病毒定义、创建和打印详细的报告及设置警报
Symantec Endpoint Protection Manager	与端点客户端通信，并且通过 Symantec Endpoint Protection Manager 控制台进行配置
Symantec Endpoint Protection	为网络计算机和非网络计算机提供病毒、防火墙、主动型威胁扫描及入侵防护
Symantec Network Access Control	为网络计算机提供网络遵从防护
LiveUpdate 服务器	能够从 Symantec LiveUpdate 服务器提取定义、特征和产品更新，并且将更新分发至客户端
中央隔离区	属于数字免疫系统的一部分，可针对启发式检测到的新病毒或无法识别的病毒提供自动响应

5. Symantec Endpoint Protection Manager 的工作方式

用户可以根据需要将客户端安装为受管客户端或非受管客户端，安装为受管客户端后，即为受管网络；安装为非受管客户端后，则为非受管网络。受管网络可充分利用网络的功能，网络上的每个客户端和服务端都可通过运行 Symantec Endpoint Protection Manager 的一台计算机进行监控、配置和更新。用户也可以从 Symantec Endpoint Protection Manager 控制台安装和升级 Symantec Endpoint Protection 与 Symantec Network Access Control 客户端。

在非受管网络中必须单独管理每台计算机，或将管理职责转交给该计算机的主要用户。信息技术资源有限或匮乏的小型网络应采用这种方法，其相关职责如下。

- (1) 更新病毒及安全风险定义。
- (2) 配置防病毒及防火墙。
- (3) 定期升级或迁移客户端软件。

提示

如果要允许用户更改客户端设置，建议最好将客户端安装在受管环境中。

在受管网络中，用户可以将客户端分成组。使用这些组可将需要相似访问级别和配置设置的客户端放在同一组，也可以选择组中指定不同的位置设置。如果客户端是从不同的位置访问网络，则可应用不同的策略。

6. Symantec Endpoint Protection Manager 的功能

使用 Symantec Endpoint Protection Manager 可执行下列操作。

- (1) 建立和强制实施安全策略。
- (2) 防止受到病毒、混合型威胁，以及安全风险（如广告软件和间谍软件）的侵害。
- (3) 利用集成的管理控制台来管理病毒防护的部署、配置、更新和报告。
- (4) 防止用户访问计算机的硬件设备，例如 USB 驱动器。
- (5) 利用集成的管理控制台来管理病毒防护、防火墙防护和入侵防护的部署、配置、更新和报告。
- (6) 管理客户端及其位置。
- (7) 标识过期的客户端，迅速应对病毒爆发并部署更新的病毒定义。
- (8) 创建和维护详细描述网络中发生的重要事件的报告。
- (9) 为连接到网络的所有用户提供针对安全威胁的高级别的防护和集成响应，此防护覆盖始终保持网络连接的远程办公人员和间歇连接到网络的移动用户。
- (10) 获得分布在网络中的所有工作站的多个安全组件的合并视图。
- (11) 对所有安全组件执行可定制且集成的安装并同时设置策略。
- (12) 查看历史记录和日志数据。

►► 20.1.2 安装 Symantec Endpoint Protection Manager

Symantec Endpoint Protection Manager 类似于 Symantec AntiVirus 企业版中的系统中心，主要用于管理 SEP 服务器和客户端，直接从光盘安装即可。Symantec Endpoint Protection Manager 引进了数据库管理技术，最多可以支持超过 5 000 个端点的网络环境。网络管理员可以通过创建不同的服务器组，实现网络负载均衡。

1. 安装要求

新一代 Symantec 计算机网络安全防御系统对目标计算机硬件和软件要求更加严格，除满足最低需求外，目标计算机上的用户账户还必须拥有远程登录和管理客户端的权限，以便实现远程部署和管理。

(1) 硬件需求

安装 Symantec Endpoint Protection Manager 的基本硬件需求如表 20-2 所示, 硬件性能的高低将直接影响到服务器的稳定性和可以支持的客户端数量。

表 20-2 Symantec Endpoint Protection Manager 基本硬件需求

组 件	x86	x64
处理器	1 GHz Intel Pentium III	Intel EM64T 的 Intel Xeon 和 Intel Pentium IV 处理器, 以及 AMD 64 位 Opteron 和 Athlon 处理器, 不支持 Itanium 处理器
内存	1 GB (建议使用 2 GB)	1 GB (建议使用 2 GB)
硬盘	2 GB (建议使用 4 GB)	2 GB (建议使用 4 GB)
显示器	Super VGA (1,024x768) 或更高分辨率的视频适配器和显示器	Super VGA (1 024x768) 或更高分辨率的视频适配器和显示器

(2) 系统和软件需求

Symantec Endpoint Protection Manager 支持以下操作系统。

Windows 2000 Server SP 3 或更高版本。

Windows XP Professional (带 Service Pack 1) 或更高版本。

Windows Server 2003 各种版本 (64 位版本必须集成 SP 1 或更高版本系统补丁)。

x64 Windows Server 2003 服务器群集。



注意:

如果要为 Symantec Endpoint Protection Manager 服务器使用 Microsoft 群集服务, 则必须在本地卷上安装 Symantec Endpoint Protection Manager 服务器。



安装 Symantec Endpoint Protection Manager 的计算机必须满足下列最低软件要求。

安装和启用 IIS 5.0 或更高版本。

Internet Explorer 6.0 或更高版本。

使用静态 IP 地址。

Microsoft SQL 2000/2005 数据库服务器 (可选)。

(3) 用户权限需求

如果要安装 Symantec 客户端软件, 用户必须具有客户端或 Windows 域的管理员权限, 并以管理员的身份登录。Symantec 软件安装程序会在计算机上启动另一个安装程序, 以便创建和启动服务并修改注册表。

如果不想为用户提供其计算机的管理权限, 可以使用“推式部署向导”远程安装 Symantec 客户端。要运行该向导, 用户必须具有安装该程序的计算机的本地管理权限。

如果是用 Active Directory 管理计算机, 可以创建组策略, 该策略将提供安装 Symantec 软件所必需的用户权限。

2. 安装 Symantec Endpoint Protection Manager

安装 Symantec Endpoint Protection Manager 之前必须确保已经安装并启动了 IIS 服务, 数据库服务器是可选的。如果网络客户端数量不超过 1 000 个, 完全可以使用 SEP 内置的嵌入式数据库; 如果客户端数量较多, 则建议安装独立的 SQL Server 数据库, 并建立相应的数据库实例。

① 插入安装光盘, 如果安装程序未自动启动, 则双击根目录下的 Setup.exe 文件, 显示如图 20-2 所示的“Symantec Endpoint Protection 安装程序”对话框。

② 单击“安装 Symantec Endpoint Protection Manager”按钮, 显示如图 20-3 所示的“欢迎使用

Symantec Endpoint Protection Manager 安装向导”对话框。除此之外，客户端用户还可以借助此向导本地安装 SEP 客户端。

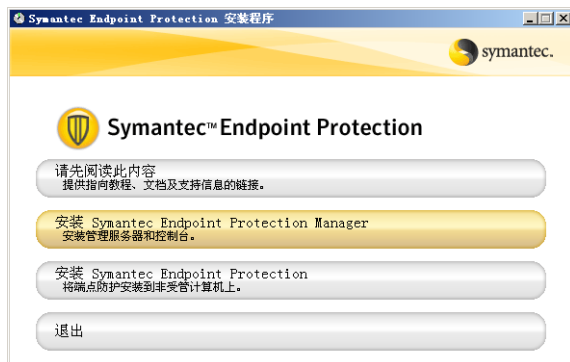


图 20-2 “Symantec Endpoint Protection 安装程序”对话框

③ 单击“下一步”按钮，显示如图 20-4 所示的“授权许可协议”对话框，选择“我接受该许可证协议中的条款”单选按钮。



图 20-3 “欢迎使用 Symantec Endpoint Protection Manager 安装向导”对话框 图 20-4 “授权许可协议”对话框

④ 单击“下一步”按钮，显示如图 20-5 所示的“目标文件夹”对话框。单击“更改”按钮可以重新选择安装目录，建议接受默认安装路径。

⑤ 单击“下一步”按钮，显示如图 20-6 所示的“选择 Web 站点”对话框。如果要在该服务器中允许 Symantec Endpoint Protection Manager IIS Web 和原有 Web 站点同时运行，则选择“使用默认 Web 站点”单选按钮；如果要将 Symantec Endpoint Protection Manager IIS Web 配置为当前服务器中唯一的 Web 站点，则选择“创建自定义 Web 站点”单选按钮。为了提高 Symantec 服务器自身的安全性，建议选择“创建自定义 Web 站点”单选按钮。



图 20-5 “目标文件夹”对话框

图 20-6 “选择 Web 站点”对话框

⑥ 单击“下一步”按钮，显示如图 20-7 所示的“准备安装程序”对话框，提示安装向导已经准备就绪。

⑦ 单击“安装”按钮开始安装，需要等待一段时间，完成后显示如图 20-8 所示的“安装向导已完成”对话框。



图 20-7 “准备安装程序”对话框

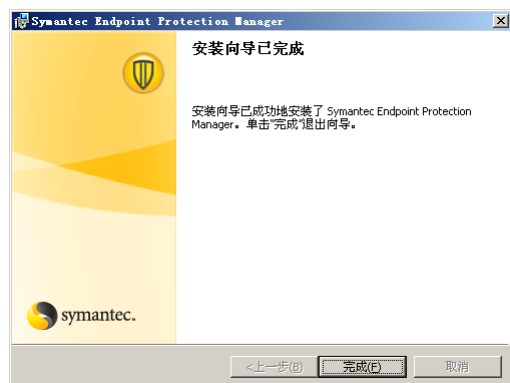


图 20-8 “安装向导已完成”对话框

⑧ 单击“完成”按钮，即可完成 Symantec Endpoint Protection Manager 的安装。

3. 配置 Symantec Endpoint Protection Manager

安装 Symantec Endpoint Protection Manager 之后，还需要根据需要进行相应配置，包括创建服务器组、设置站点名称、管理员密码、客户端安装方式，以及制作客户端安装包等。默认情况下，关闭安装向导后将自动启动“管理服务器配置向导”。如果没有启动，则按照如下方法打开并配置。

① 单击“开始”→“所有程序”→“Symantec Endpoint Protection Manager”→“管理服务器配置向导”选项，显示如图 20-9 所示的“欢迎使用管理服务器配置向导”对话框。此处提供“简单”和“高级”两种配置类型，区别在于“简单”模式下只能使用嵌入式数据库，支持不多于 100 个的客户端，并且无法定义服务器通信端口及站点名称。安全性相对较低，因此建议选择“高级”单选按钮。

② 单击“下一步”按钮，指定该管理服务器管理的客户端数量，如图 20-10 所示，本例选择“500 到 1000 台”单选按钮。需要注意的是，如果客户端数量少于 100 个，则可以使用该模式配置安全性较高的管理服务器。



图 20-9 “欢迎适用管理服务器配置向导”对话框



图 20-10 指定客户端数量

③ 单击“下一步”按钮，在显示的对话框中选择安装类型，如图 20-11 所示，选择“安装我的第一个站点”单选按钮即可。无论使用单点管理模式还是使用服务器群集模式，都必须首先安装并配

置第 1 个管理服务器站点。

④ 单击“下一步”按钮，在显示的对话框中选择管理服务器名称和通信端口，如图 20-12 所示。在“服务器名称”文本框中输入 Symantec 管理服务器的名称，便于客户端的查找和确认。“服务器端口”和“Web 控制台”端口均保留默认即可，“服务器数据文件夹”用于存储服务器备份、复制日志和其他文件。如果此目录不存在，安装程序会创建它。



图 20-11 选择安装类型



图 20-12 设置服务器名称和通信端口

⑤ 单击“下一步”按钮，在显示的对话框中设置站点名，如图 20-13 所示。在“站点名”文本框中输入适当名称，如 SEP。

⑥ 单击“下一步”按钮，在显示的对话框中设置加密密码，如图 20-14 所示。在 SEP 安全防御系统中，管理服务器和客户端之间的通信均是被加密的，以确保传输过程中的安全。在“简单”模式下配置服务器时，加密密码会设置为与为管理员账户配置的密码相同。



图 20-13 设置站点名



图 20-14 设置加密密码



必须妥善保管此密码。创建数据库之后将不能更改或恢复密码。当没有可还原的备份数据库时，必须输入此密码，才能进行灾难恢复。



⑦ 单击“下一步”按钮，在显示的对话框中选择适用的数据库类型，如图 20-15 所示。如果客

户端数量不超过 5 000 个, 则建议选择默认的“嵌入式数据库”单选按钮, 以避免不必要的兼容性问题, 这里保留默认。如果要实现服务器集群, 则必须选择“Microsoft SQL Server”单选按钮。

⑧ 单击“下一步”按钮, 在显示的对话框中创建系统管理员账户, 如图 20-16 所示。默认账户名称为“admin”, 在“密码”和“确认密码”文本框中输入管理员账户的登录密码即可。



图 20-15 选择数据库类型



图 20-16 创建管理员账户及密码

⑨ 单击“下一步”按钮, 开始创建嵌入式数据库, 大约需要几分钟的时间。完成后显示如图 20-17 所示的“管理服务器配置向导已完成”对话框, 提示完成此向导后并不会在本地计算机上安装 SEP 客户端。如果选择“是”单选按钮, 则单击“完成”按钮将自动启动“迁移和部署向导”, 以完成客户端远程安装包的创建等工作。

⑩ 单击“完成”按钮完成管理服务器配置向导。

4. 迁移和部署向导

迁移和部署向导主要用来帮助管理员完成客户端的部署, 或者将客户端从旧版本 Symantec AntiVirus 迁移到 Symantec Endpoint Protection 管理平台。可以在完成“管理服务器配置向导”后立即开始部署, 也可以按照如下方法完成。

① 单击“开始”→“所有程序”→“Symantec Endpoint Protection Manager”→“迁移和部署向导”选项, 打开如图 20-18 所示“欢迎使用迁移和部署向导”对话框。



图 20-17 “管理服务器配置向导已完成”对话框



图 20-18 “欢迎使用迁移和部署向导”对话框

② 单击“下一步”按钮，在显示的对话框中选择要执行的操作，如图 20-19 所示。如果需要采用“推”方式远程部署客户端或者创建客户端安装程序，则选择“部署客户端”单选按钮；如果要进行服务器迁移，则选择“从旧版本 Symantec AntiVirus 迁移”单选按钮。本例选择“部署客户端”单选按钮。

③ 单击“下一步”按钮，在显示的对话框中指定要部署的客户端组，如图 20-20 所示。客户端组是对客户端进行统一管理的常用工具，默认情况下，Symantec Endpoint Protection Manager 已经提供了一个名为“temporary”的组，默认情况下所有采用“拉”方式安装的客户端都将被添加到该组中。选择“指定您要部署客户端的新组名”单选按钮并在文本框中输入组名，则通过此向导部署的客户端将自动加入该组。



图 20-19 选择要执行的操作

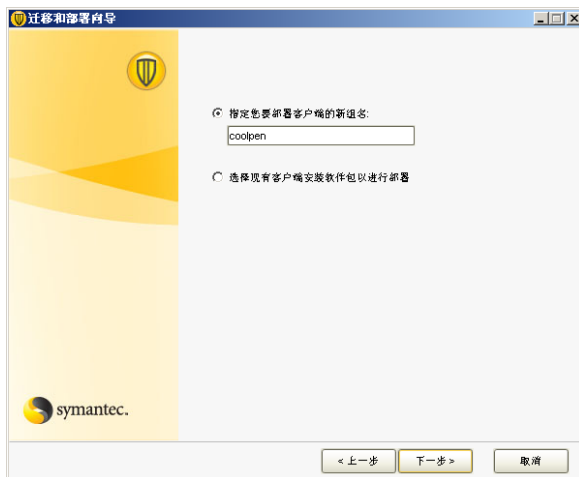


图 20-20 指定要部署的客户端组

④ 单击“下一步”按钮，在显示的对话框中定制该客户端安装包中提供的保护功能，如图 20-21 所示，通常保留默认即可。如果客户端使用 Outlook 管理电子邮箱，也可以选中“Microsoft Outlook 扫描程序”复选框。

⑤ 单击“下一步”按钮，在显示的对话框中定制安装包的类型及安装方式，如图 20-22 所示。使用默认配置创建的安装程序将适用于 32 位客户端，文件格式为.EXE，并且在无人参与情况下完成安装。单击“浏览”按钮，可以设置存储安装程序的目标文件夹。注意，此处的文件夹路径必须全部用英文表示，即必须遵循表 20-3 所示的国际化准则。



图 20-21 定制安装包功能

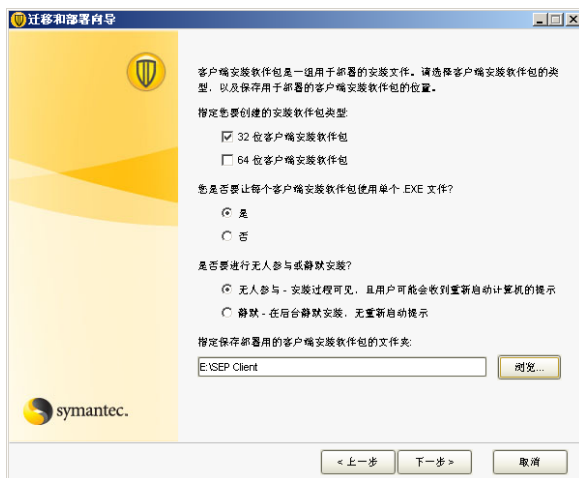


图 20-22 定制安装包的类型及安装方式

表 20-3 国际化命名准则

组 件	命名准则
计算机名、域名及工作组名	支持非英文字符时的限制如下。 <ul style="list-style-type: none">➤ 对于那些使用双字节字符集或 hi-ASCII 字符集的名称，网络审核功能可能无法正常工作➤ 在 Symantec Endpoint Protection Manager 控制台或 Symantec Endpoint Protection 客户端用户界面中双字节字符集名称或 hi-ASCII 字符集名称可能无法正常工作➤ 较长的双字节或 hi-ASCII 字符集主机名不能长于 NetBIOS 允许的长度，如果主机名长于 NetBIOS 允许的长度，则 Symantec Endpoint Protection Manager 控制台中不显示“主页”、“监视器”和“报告”页面➤ 以双字节或 hi-ASCII 字符名称命名的客户端计算机用作组更新提供程序时无法工作
在下列情况下请只使用英文字符	<ul style="list-style-type: none">➤ 将客户端软件包部署到远程计算机➤ 在 Symantec Endpoint Protection Manager 的服务器配置向导页中定义服务器数据文件夹➤ 定义 Symantec Endpoint Protection Manager 的安装路径➤ 在将客户端部署到远程计算机时定义凭据➤ 定义组名称，可以为名称中包含非英语字符的组创建客户端软件包。但是当组名中包含非英语字符时，可能无法使用“推送部署向导”部署客户端软件包➤ 将非英语字符推送至客户端，在服务器端生成的某些非英语字符在客户端用户界面中可能无法正确显示。例如，双字节字符集位置名称在以非双字节字符集命名的客户端上无法正确显示
客户端计算机上的“用户信息”对话框	安装完导出的软件包之后，在客户端上的“用户信息”对话框中提供反馈时，勿使用双字节字符或 hi-ASCII 字符
启用 SQL Server 中的 I18n 支持	使用 SQL Server 数据库的双字节、hi-ASCII 或混合语言环境需要启用批处理模式，管理员可以在 SQL Server 中启用 I18n 支持

⑥ 单击“下一步”按钮，在显示的对话框中设置是否立即部署到远程客户端，如图 20-23 所示。如果选择“是”单选按钮，则完成向导后将立即开始在远程计算机上安装 SEP 客户端，这里选择“否，只要创建即可，我稍后会部署”单选按钮。

⑦ 单击“完成”按钮，关闭“迁移和部署向导”即可。默认情况下将自动启动“Symantec Endpoint Protection Manager 控制台”，显示如图 20-24 所示的登录窗口。

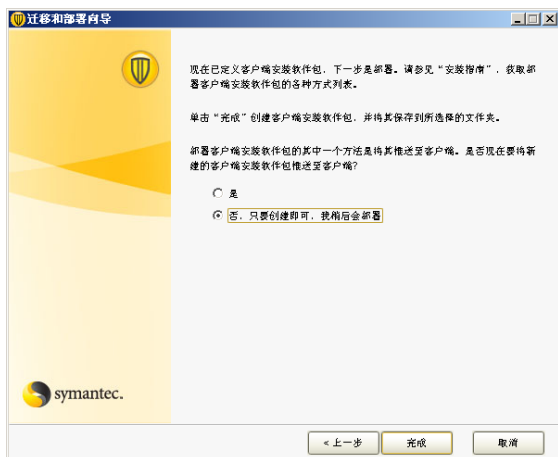


图 20-23 设置是否立即部署客户端



图 20-24 登录窗口

5. 安装 Symantec Endpoint Protection Manager Web 控制台

默认安装的 Symantec Endpoint Protection Manager 通过 MMC 控制台管理，如今网络中的许多网络设备都支持远程 Web 管理。为便于统一维护，网络管理员也可以根据需求选择安装 Symantec Endpoint Protection Manager Web 控制台，需要注意的是，这种控制台的运行需要 Java 的支持。如果管理计算机上没有安装 Java 或版本不正确，均无法实现远程管理。



注意：

如果从远程管理控制台导出客户端安装软件包，就会在运行远程管理控制台的计算机创建软件包。另外，安装用于故障转移或负载平衡的服务器时需要在这些计算机中安装管理控制台。



在要进行远程管理 Symantec Endpoint Protection Manager 的计算机中打开 IE 浏览器，在地址栏中输入地址 [http://计算机名或 IP 地址:9090](http://计算机名或IP地址:9090)。按回车键，打开如图 20-25 所示的窗口，9090 是在安装过程中使用的默认 Web 控制台端口。当前计算机的安全级别设置过高，或者没有将 Symantec Endpoint Protection Manager 服务器站点添加到信任区，则可能无法完全显示该信息。单击“此处”超级链接，即可开始下载并安装，安装过程中可能需要用户修改本地计算机安全等级，以允许安装 Active X 插件。

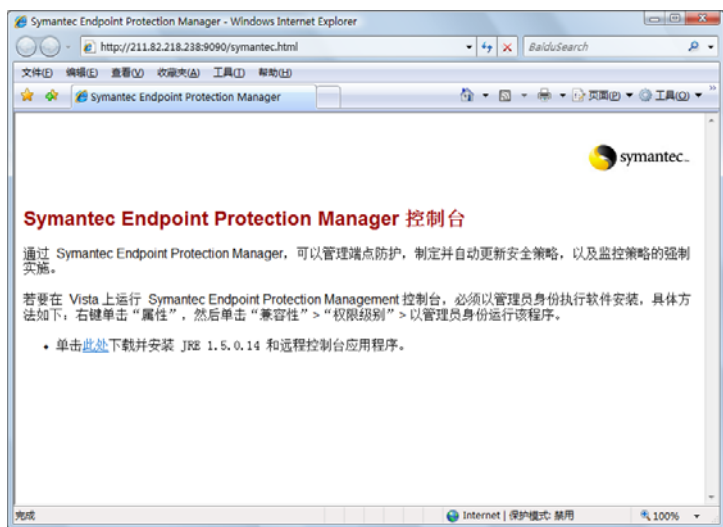


图 20-25 安装 Web 控制台窗口

20.2 部署 Symantec Endpoint Protection 客户端

SEP 客户端可分为非受管和受管客户端，其中受管理客户端可以通过 Symantec Endpoint Protection Manager 远程部署等方式安装，也可以在客户端上使用管理服务器创建的安装包安装。安装完成后将自动添加到指定组中，并接受服务器的统一管理；非受管客户端则可以通过安装光盘完成，虽然同样可以被添加到服务器控制台中，但不接受服务器的管理。需要注意的是，Symantec Endpoint Protection 在安装过程中需要至少 700 MB 的硬盘空间。如果空间不足，将导致安装失败。

20.2.1 部署受管理客户端

用户可以通过如下几种方法部署接受 Symantec Endpoint Protection Manager 服务器安装的客户端。

- (1) 迁移和部署向导的“推”式安装。
- (2) 客户端映射网络驱动器安装。
- (3) 使用“查找非受管计算机”部署。
- (4) 手动安装。
- (5) 使用 Altiris 安装和部署软件安装。
- (6) 使用第三方产品安装。

1. 迁移和部署向导的“推”式安装

在创建客户端安装包过程中可以同时定制完成的安装程序部署到客户端，也可以选择创建完成

后保存到服务器上，需要部署时通过“迁移和部署向导”完成。需要注意的是，Windows Vista 操作系统中的用户访问控制（UAC）功能禁止本地管理账户远程访问远程管理共享，如 C\$ 和 Admin\$，使用该方式部署时应将其关闭。使用现有安装包部署受管理客户端的操作步骤如下。

① 启动“迁移和部署向导”，连续单击“下一步”按钮。直至显示如图 20-26 所示的提示选择部署方式的对话框，选择“选择现有客户端安装软件包以进行部署”单选按钮。

② 单击“完成”按钮，显示如图 20-27 所示的“推式部署向导”对话框。单击“浏览”按钮选择已经创建完成的安装程序所在目录，在“指定并行部署数量上限”文本框中输入相应的值（以管理服务器性能而定），默认为 10 个。



图 20-26 选择部署方式

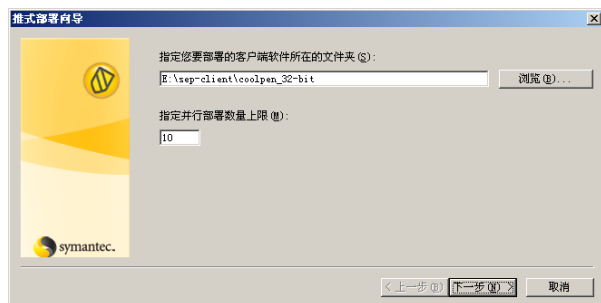


图 20-27 “推式部署向导”对话框

③ 单击“下一步”按钮，显示如图 20-28 所示的选择可用计算机对话框。在“可用计算机”下拉列表框中展开“Microsoft Windows Network”→“工作组名或域名”，并选择要作为客户端的计算机，单击“添加”按钮添加。

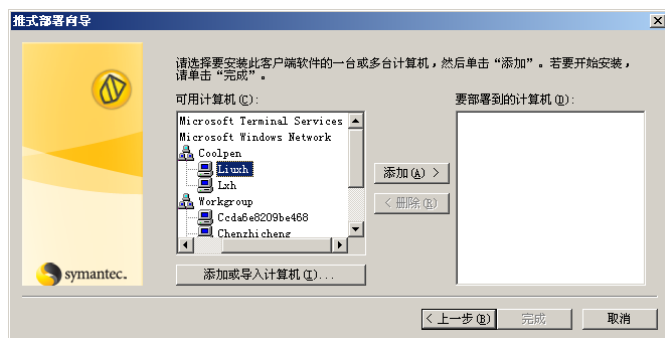


图 20-28 选择可用计算机



提示

如果“可用计算机”下拉列表框中没有显示要部署的客户端计算机，则单击“添加或导入计算机”按钮，打开如图 20-29 所示的“添加或导入计算机”对话框。选择“IP 地址或主机名”和“IP 地址”单选按钮，并输入计算机 IP 地址，单击“添加”按钮将其添加到“添加的计算机”下拉列表框中。单击“确定”按钮并按照要求提供相应登录凭据，即可添加到“要部署到的计算机”列表框中”。另外，还可以选择“含有主机名及 IP 地址的文件”单选按钮，并单击“浏览”按钮直接导入编辑的客户端计算机列表。

④ 单击“添加”按钮，显示如图 20-30 所示的“远程客户端验证”对话框，在“用户名”和“密码”文本框中输入远程登录目标计算机时使用的账户信息。单击“确定”按钮将其添加到“要部署到

的计算机”列表框中，重复操作可以同时添加多个客户端。

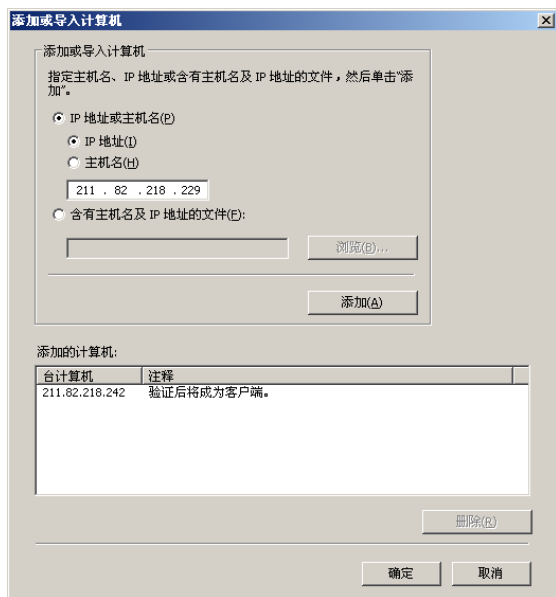


图 20-29 “添加或导入计算机”对话框

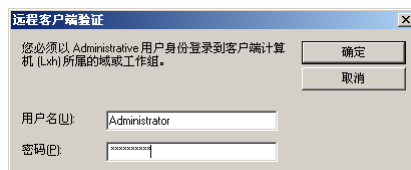


图 20-30 “远程客户端验证”对话框



提示

如果远程计算机中没有启用网络共享，或者启用了 Windows 防火墙，则此处可能无法正常添加计算机，会出现“无任何网络提供程序接受指定的网络路径”类似信息，此时只需启用防火墙和系统共享（尤其是系统默认共享）即可。如果目标计算机是 Windows Server 2008 Server Core 系统，则可以执行如下命令将共享添加到 Windows 防火墙允许的应用程序中：

```
netsh firewall set service fileandprint enable
```

⑤ 添加所有需要部署的客户端后，单击“完成”按钮开始安装，显示如图 20-31 所示的“远程客户端安装状态”对话框。

⑥ 安装完成后，“全部取消”按钮将变为“关闭”按钮，单击此按钮即可关闭对话框，显示如图 20-32 所示的“推式部署向导”对话框，提示是否查看部署日志。如果并发部署的客户端较多，则可能由于服务器性能导致部分客户端无法正常完成，此时即可通过部署日志确定完成情况。

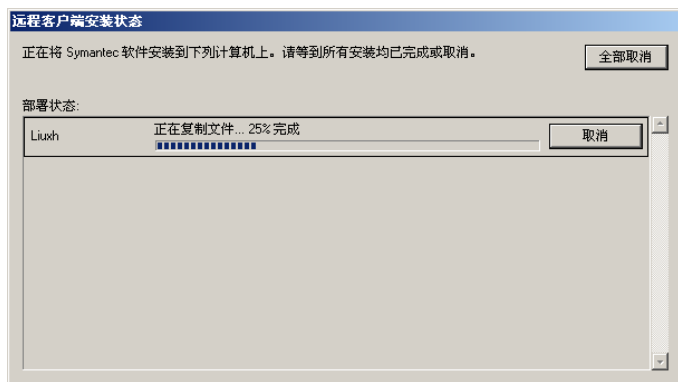


图 20-31 “远程客户端安装状态”对话框



图 20-32 “推式部署向导”对话框

至此，管理服务器上的远程部署工作已完成，客户端将开始自动安装。安装完成后将提示用户是否立即重新启动计算机和更新病毒库，按照要求操作即可。

2. 通过映射网络驱动器安装

将已经创建的客户端安装程序保存到服务器的某个目录中，并共享该目录，客户端即可通过局域网访问该安装包。通过将其映射为网络驱动器，即可通过网络安装。安装过程由安装包自身的定制功能和安装模式决定，通常无需用户人工干涉。与通过“迁移和部署向导”方式类似，此处不复赘述。

在 Symantec Endpoint Protection 客户端软件安装期间，映射驱动器会暂时断开，这是已知且可预期的操作。在安装 Symantec Network Access Control 客户端软件时，不会执行此项操作。

3. 使用“查找非受管计算机”部署

管理员可使用 Symantec Endpoint Protection Management 控制台中的“查找非受管计算机”部署客户端软件，用其可以扫描没有运行客户端软件的客户端计算机，然后在这些计算机中安装客户端软件。

(1) 登录到“Symantec Endpoint Protection Management 控制台”，单击左窗格中的“客户端”按钮，显示如图 20-33 所示的“查看客户端”窗口。在“查看客户端”树中单击分组名称，即可查看当前分组中的客户端。

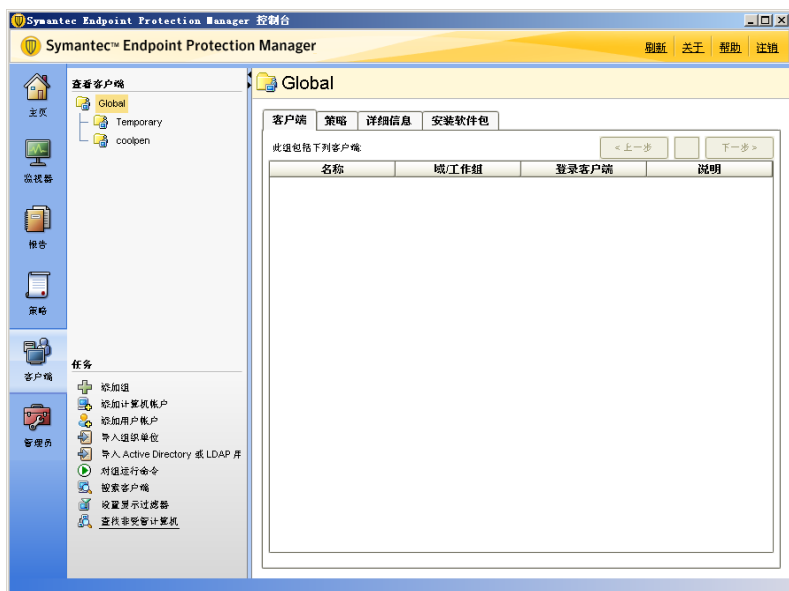


图 20-33 “查看客户端”窗口

(2) 在“任务”列表框中单击“查找非受管计算机”超级链接，显示如图 20-34 所示的“查找非受管计算机”对话框。在“搜索依据”选项组中选择“IP 地址范围”单选按钮，并设置适当的起止 IP 地址；在“登录证书”选项组中输入登录客户端计算机的凭证及所在工作组或域。单击“立即搜索”按钮开始搜索，搜索结果将显示在“非受管计算机”和“未知的计算机”列表框中，默认显示“非受管计算机”选项。



提示

“非受管计算机”列表框中显示的是安装非受管客户端的计算机，或者曾经安装过客户端，但现在已经卸载的；“未知的计算机”列表框中显示的是当前网络中所有没有部署 SEP 客户端的计算机。

(3) 选中要部署的对象，并在“安装”选项组中设置相应的安装选项。在“客户端安装软件包”下拉列表框中选择适用的安装包类型，包括 32 位和 64 位两种，分别用于不同的系统平台。“安装设置”选项保留系统默认值即可。在“功能”下拉列表框中可以定制客户端的基本功能，选择“Symantec Endpoint Protection 的所有功能”选项。

(4) 默认情况下,被部署的客户端将自动分配到“Temporary”组中。单击“更改”按钮,打开如图 20-35 所示的“网络搜索选项”对话框。选择要添加到的组(如 coolpen),然后单击“确定”按钮。



图 20-34 “查找非受管计算机”对话框

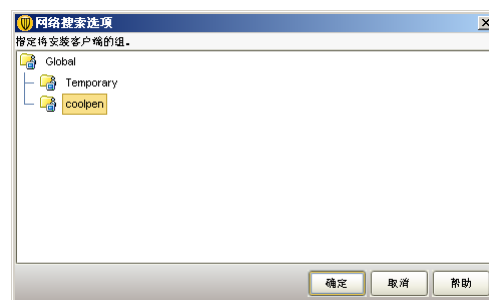


图 20-35 “网络搜索选项”对话框

(5) 准备就绪后,在“查找非受管计算机”对话框中单击“开始安装”按钮,开始将 SEP 客户端“推”安装到目标计算机中。完成后显示如图 20-36 所示的结果,“部署状态”显示为“成功”即表明客户端安装成功。在“推”安装过程中客户端不会提示任何信息,在安装完成后才会提示用户升级病毒库。



图 20-36 部署成功

4. 使用 Altiris 安装和部署软件安装

用户可以使用 Altiris (现在为 Symantec 的一部分) 安装和部署 Symantec 客户端软件, Altiris 提

提供一个免费的 Symantec Endpoint Protection 集成组件，该组件提供默认安装功能、集成的客户端管理，以及高级别报告功能。

Altiris 软件使得信息技术组织可以管理、保护并维护不同种类的 IT 资产，它还支持软件提交、补丁程序管理、配置，以及其他多项管理功能。该软件可帮助 IT 改善服务来推动商业目标的实现、实现经得起审核的安全性、自动执行任务，并且降低管理的成本和复杂性。

5. 使用第三方产品安装

Symantec 客户端软件支持第三方安装方式，用户可以使用这些方式部署客户端软件，并且可以进行大规模且无人值守安装。常用的安装 SEP 客户端的产品有 Microsoft Active Directory、Tivoli、Microsoft Systems Management Server (SMS)，以及 Novell ZENworks 等，其中 Active Directory 和 SMS 最为常用。并且由于是微软公司的产品，所以可以和 Windows 完全集成。推荐使用，当然用户必须熟悉相应的操作方式。

20.2.2 部署非受管客户端

Symantec Endpoint Protection 非受管客户端的部署通常借助安装光盘完成，安装过程并不复杂，而对于 Windows Server 2008 Server Core 系统而言，由于系统仅提供了命令行界面，所以必须借助相关命令完成客户端的部署。对于不熟悉命令操作的网络管理员而言，可能会有些难度。

1. 部署 Windows Vista 非受管客户端

以 Windows Vista 为例，通过安装光盘部署 Symantec Endpoint Protection 非受管客户端的操作步骤如下。

① 插入 Symantec Endpoint Protection 安装光盘，光盘自动运行，显示如图 20-37 所示的“Symantec Endpoint Protection 安装程序”对话框。如果未能自动运行，则在资源管理器中运行光盘根目录下的 setup.exe 文件。

② 单击“安装 Symantec Endpoint Protection”按钮启动 Symantec Endpoint Protection 安装向导，需要接受相关的许可协议。连续单击“下一步”按钮，显示如图 20-38 所示的“客户端类型”对话框，选择“非受管客户端”单选按钮即可。

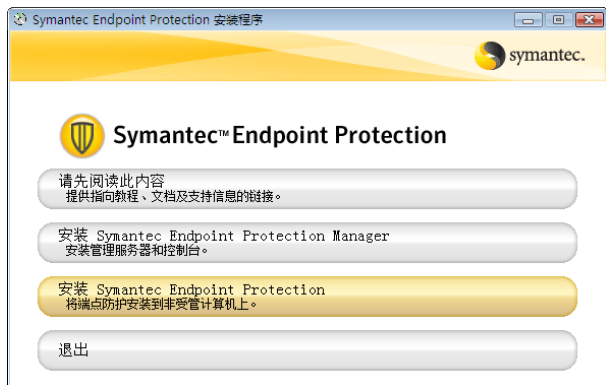


图 20-37 “Symantec Endpoint Protection 安装程序”对话框



图 20-38 “客户端类型”对话框

③ 单击“下一步”按钮，显示如图 20-39 所示的“安装类型”对话框，系统默认选择“典型”单选按钮。也可以根据需要进行选择“自定义”单选按钮，并选择要安装的安全防护功能。建议使用系统默认设置。

④ 单击“下一步”按钮，显示如图 20-40 所示的“准备安装程序”对话框。其中提示向导已准备好，可以开始安装。



图 20-39 “安装类型”对话框



图 20-40 “准备安装程序”对话框

⑤ 单击“安装”按钮开始安装，由于 SEP 客户端中集成的功能和组件比较多，因此可能需要较长的时间。安装完成后显示如图 20-41 所示的“InstallShield 向导完成”对话框。

⑥ 单击“完成”按钮，关闭安装向导。默认情况下，将自动启动 Liveupdate 向导更新病毒库。最后会显示如图 20-42 所示的“重新启动通知”提示框，提示必须重新启动计算机方可使 Symantec Endpoint Protection 的配置生效。

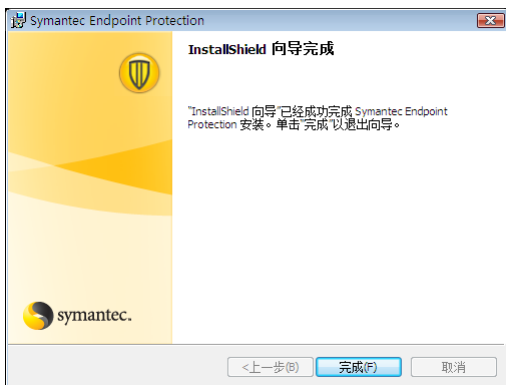


图 20-41 “InstallShield 向导完成”对话框



图 20-42 “重新启动通知”提示框

⑦ 重新启动计算机后，即可完成非受管客户端的安装。Windows 2000/XP/2003/2008 系统的安装步骤与此类似，这里不再赘述。

2. 在 64 位 Windows Server 2008 Server Core 中安装非受管 SEP 客户端

(1) 插入 Symantec Endpoint Protection 安装光盘，打开光盘根目录，执行如下命令进入安装程序所在目录：

```
cd SEPWIN64\X64
```

(2) 执行如下命令：

```
vcredist_x64.exe
```

(3) 返回安装光盘的根目录，输入 Setup.exe 后按回车键启动安装向导，借助该向导可顺利完成 64 位 SEP 客户端的部署。

提示 如果是 32 位 Windows Server 2008 Server Core 系统的计算机，则直接在命令提示符窗口中打开安装光盘根目录，运行 setup.exe 文件即可启动安装向导。

20.3 升级病毒库

杀毒软件根据提取的病毒特征来判断文件是否为病毒程序，升级病毒库就是不断地更新能够识别的病毒特征，增强杀毒软件与系统应用程序之间的兼容性。通常情况下，非受管客户端将每天自动从 Symantec LiveUpdate 站点下载病毒库。在新一代 Symantec 安全防御系统中新增了 LiveUpdate 管理服务器，主要为大型网络（超过 5 000 个端点）提供客户端病毒库升级管理。

20.3.1 安装 LiveUpdate 管理工具

在安装 LiveUpdate 管理工具之前，必须首先在服务器上安装 Java SE 程序；否则无法安装。可以从 Java 官方网站下载该程序，网址为 <http://www.java.com>。

① 运行 Symantec Endpoint Protection 的第 2 张光盘，显示如图 20-43 所示的“Symantec Endpoint Protection 安装程序”窗口。

② 单击“安装 LiveUpdate Administrator”按钮，启动 Symantec LiveUpdate Administrator 安装向导，显示如图 20-44 所示的“欢迎使用 Symantec LiveUpdate Administrator InstallShield Wizard”对话框。

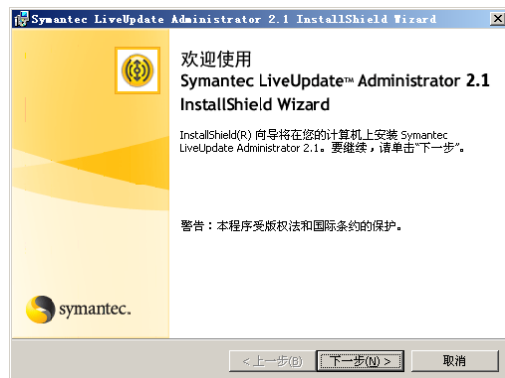


图 20-43 “Symantec Endpoint Protection 安装程序”窗口 图 20-44 “欢迎使用 Symantec LiveUpdate Administrator InstallShield Wizard”对话框

③ 单击“下一步”按钮，显示如图 20-45 所示的“许可证协议”对话框。其中要求阅读并接受许可证协议，选择“我接受该许可证协议中的条款”单选按钮。

④ 单击“下一步”按钮，显示如图 20-46 所示的“目的地文件夹”对话框。在其中可以更改安装路径，也可以使用默认值。

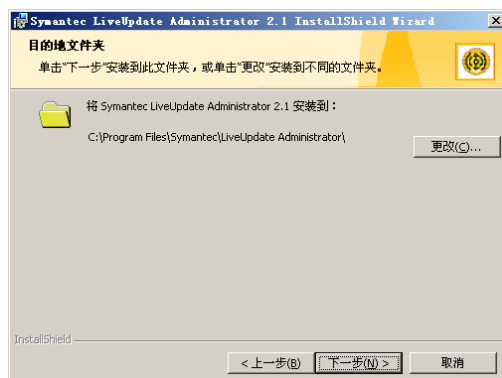
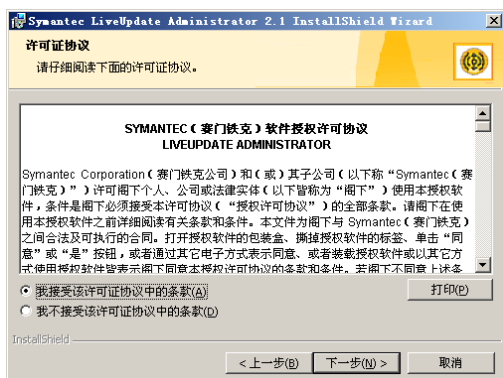


图 20-45 “许可证协议”对话框

图 20-46 “目的地文件夹”对话框

⑤ 单击“下一步”按钮，显示如图 20-47 所示的“管理更新”对话框。在其中设置存储下载更新的路径，可以使用默认设置，也可以指定其他路径。

⑥ 单击“确定”按钮，显示如图 20-48 所示的“用户安装程序”对话框。在其中设置管理员的用户名、密码和电子邮件地址，该账户用来管理 LiveUpdate。

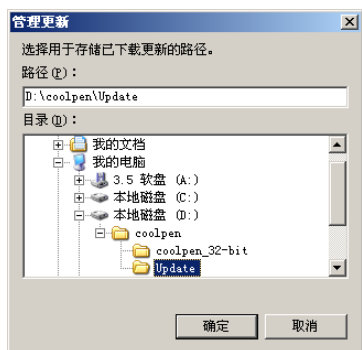


图 20-47 “管理更新”对话框

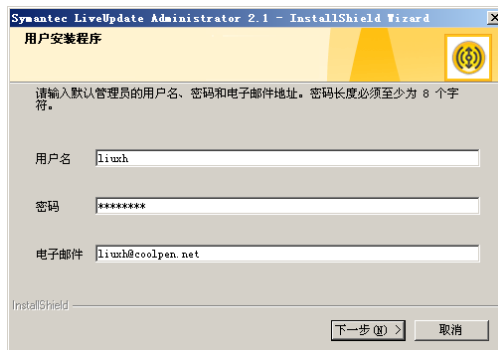


图 20-48 “用户安装程序”对话框

⑦ 单击“下一步”按钮，显示如图 20-49 所示的“已做好安装程序的准备”对话框，提示已准备开始安装。

⑧ 单击“下一步”按钮，开始安装 LiveUpdate 程序，安装完成后显示如图 20-50 所示的“InstallShield 向导完成”对话框。

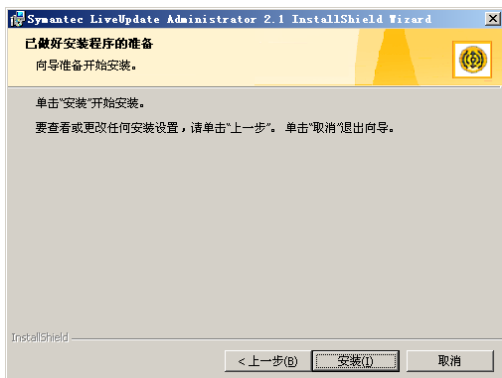


图 20-49 “已做好安装程序的准备”对话框

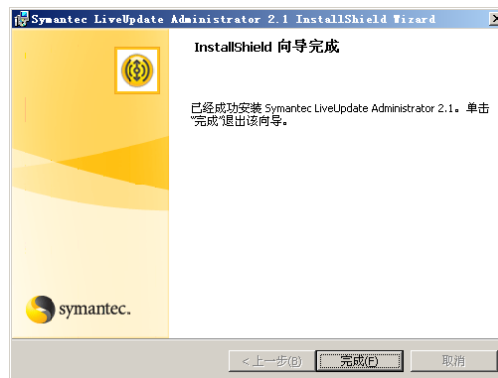


图 20-50 “InstallShield 向导完成”对话框

⑨ 单击“完成”按钮，安装完成 LiveUpdate 管理工具。

20.3.2 配置更新

Symantec LiveUpdate Administrator 安装完成以后，需要根据网络中已安装的 Symantec 产品情况添加需要下载更新的产品。

1. 登录 Symantec LiveUpdate Administrator

(1) 单击“开始”→“所有程序”→“Symantec LiveUpdate Administrator”→“LiveUpdate Administrator 2.1”选项，显示如图 20-51 所示的登录窗口，分别在“用户”和“密码”文本框中键入安装时设置的管理员用户名和密码。

(2) 单击“登录”按钮登录，显示如图 20-52 所示的“Symantec LiveUpdate Administrator”窗口，在其中可以查看最近的活动，以及系统信息。

2. 配置 LiveUpdate

在“配置”窗口中可以添加要更新的 Symantec 产品并配置下载服务器等。

添加 Symantec 产品的操作步骤如下。

① 在“Symantec LiveUpdate Administrator”窗口中单击“配置”按钮，显示如图 20-53 所示的“配置 - 我的 Symantec 产品”窗口，在其中可以添加要更新的产品。

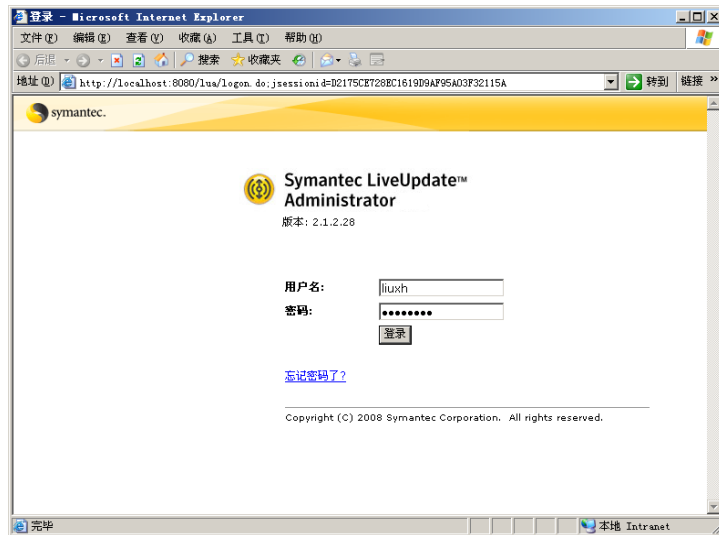


图 20-51 登录窗口

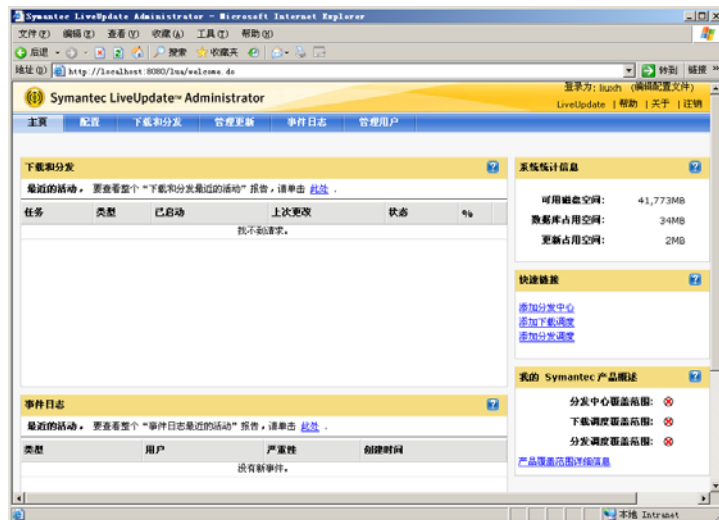


图 20-52 “Symantec LiveUpdate Administrator” 窗口



图 20-53 “配置 - 我的 Symantec 产品” 窗口

② 单击“添加新产品”按钮，显示如图 20-54 所示的“添加到我的 Symantec 产品”窗口。在“产品线”列表框中可以选择要添加的产品，这里选择“Symantec Endpoint Protection”。

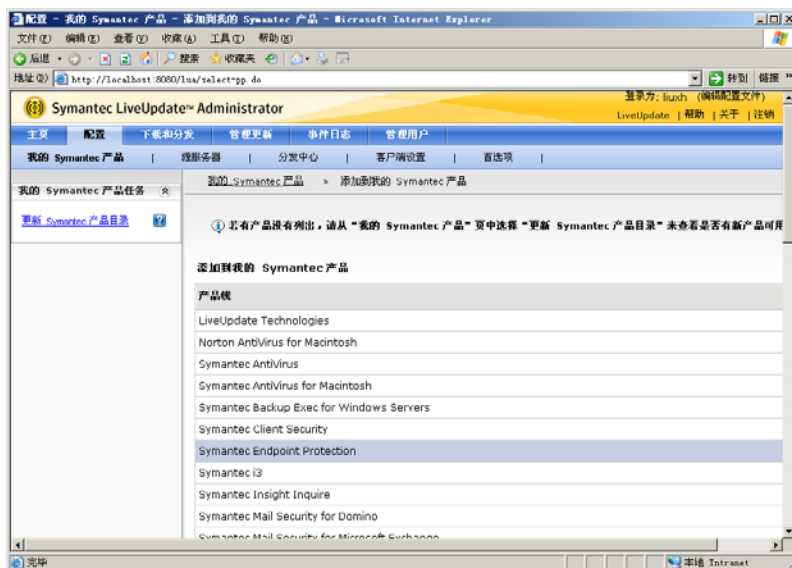


图 20-54 “添加到我的 Symantec 产品”窗口

③ 在窗口下方的“所有产品”列表框中选择要添加的产品版本，如图 20-55 所示，这里选择“Symantec Endpoint Protection v11.0 中文版（简体）”。

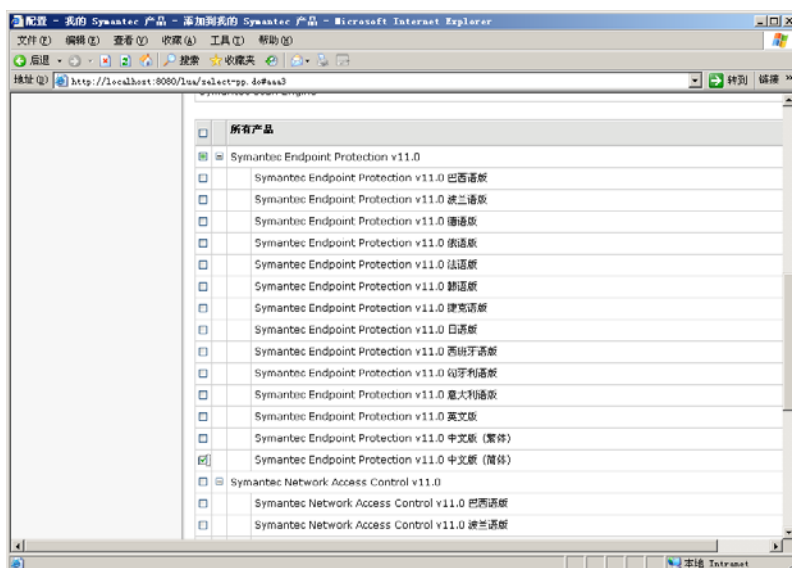


图 20-55 选择产品版本

④ 单击“确定”按钮，添加成功一个 Symantec 产品，如图 20-56 所示。如果网络中还安装有其他 Symantec 产品，也可以在此处一并添加。

配置源服务器的操作步骤如下。

在“配置”窗口中单击“源服务器”按钮，显示的“源服务器”窗口，如图 20-57 所示。在其中可以配置 Symantec 产品的更新下载服务器，默认从 Symantec 的 LiveUpdate 服务器上下载。

如果网络中已部署有 LiveUpdate 服务器，则可从本地的 LiveUpdate 服务器上下载，以节省 Internet 带宽。单击“添加”按钮，显示如图 20-58 所示的“新建源服务器”窗口，在其中添加本地网络中的 LiveUpdate 地址。

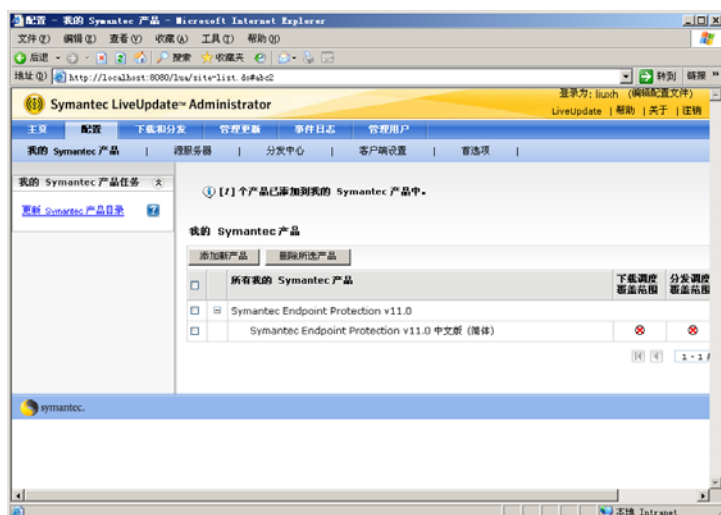


图 20-56 已添加的 Symantec 产品

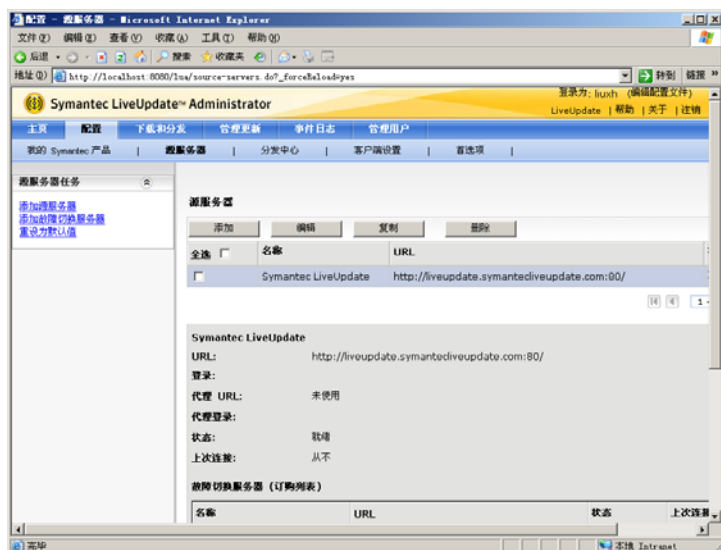


图 20-57 “源服务器”窗口

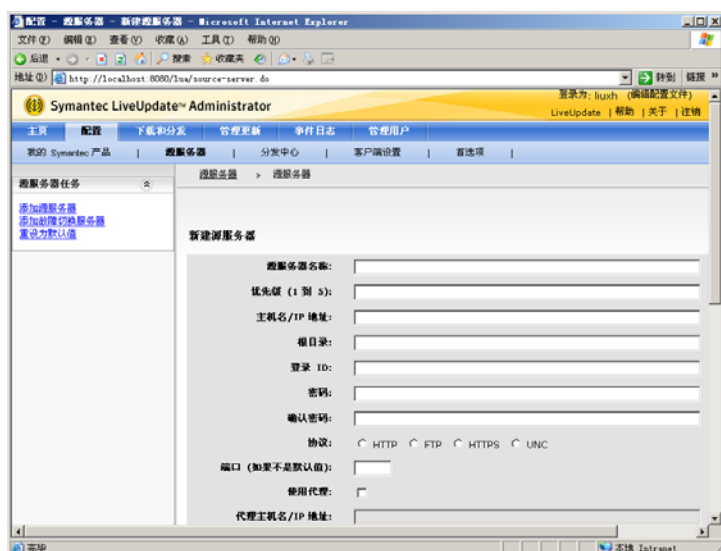


图 20-58 “新建源服务器”窗口

3. 下载和分发

添加下载调度的操作步骤如下。

① 单击“下载和分发”按钮，显示如图 20-59 所示的“下载和分发”窗口，在其中添加产品更新下载计划。

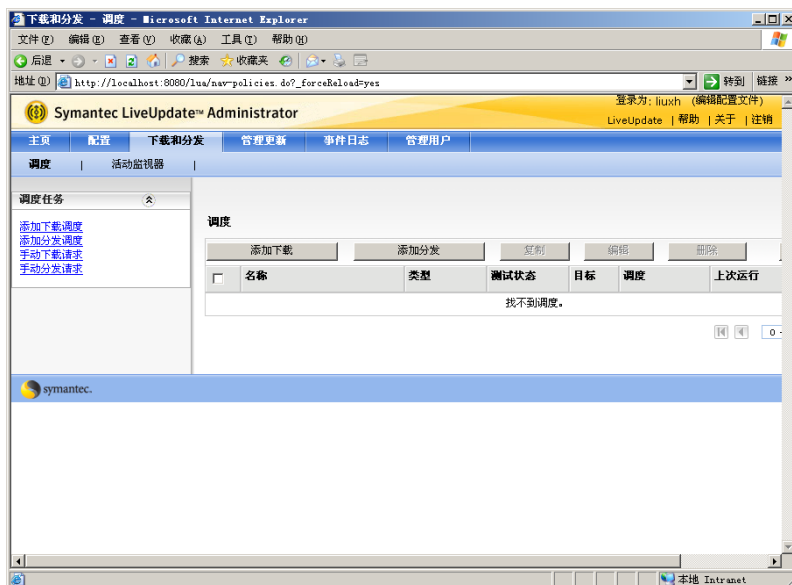


图 20-59 “下载和分发”窗口

② 单击“添加下载”按钮，显示如图 20-60 所示的“添加下载调度”窗口，在其中添加下载调度计划。在“下载调度名称”文本框中输入一个名称，在“状态”下拉列表框中选择“已启用”选项。

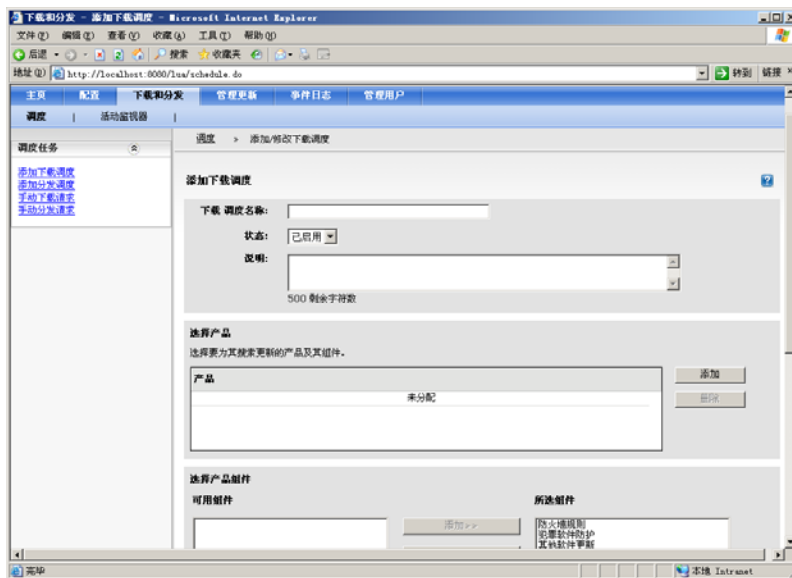


图 20-60 “添加下载调度”窗口

③ 在“选择产品”选项区域中选择要下载产品对应的复选框。单击“添加”按钮，显示如图 20-61 所示的“选择要添加的产品”窗口，在其中选中要添加的产品即可。

④ 单击“添加”按钮，将所选择的产品添加到“添加下载调度”窗口中。然后在“选择产品组件”选项组中选择要添加的组件，并在“选择调度”选项组中选择计划的执行频率。

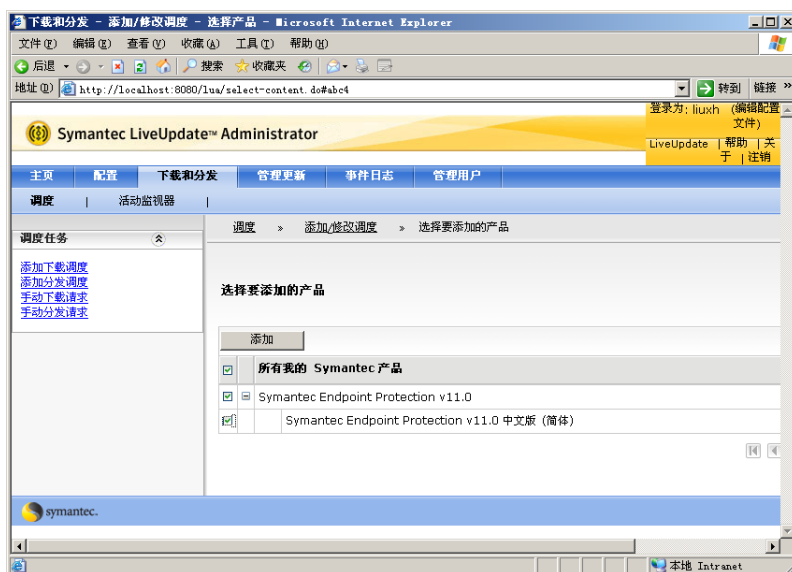


图 20-61 “选择要添加的产品”窗口

- ⑤ 完成后单击“确定”按钮，添加完成一个下载调度，如图 20-62 所示。

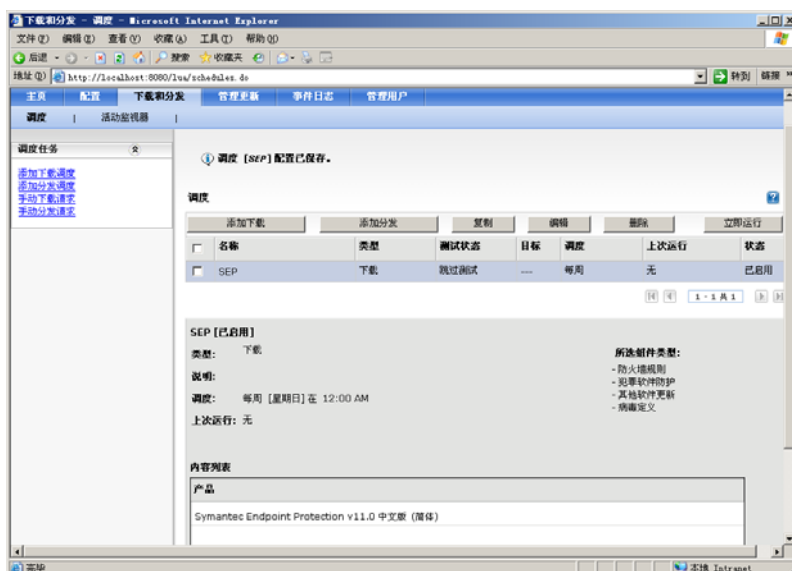


图 20-62 添加完成一个下载调度

- ⑥ 如果要立即运行下载调度，以下载更新，则选择调度名称。单击“立即运行”按钮，显示“活动监视器”窗口。在列表框中显示已下载和正在下载的组件，如图 20-63 所示。

当更新下载完成以后，客户端就可以将更新分发到各个客户端。

分发用于向客户端安装 Symantec 产品更新，可以创建分发计划定期向客户端安装更新，也可以手动向客户端分发。添加一个分发调度的操作步骤如下。

- ① 在“下载和分发”窗口中单击“添加分发”按钮，显示如图 20-64 所示的“添加分发调度”窗口。在“分发调度名称”文本框中输入一个名称，在“状态”下拉列表框中选择“已启用”选项。
- ② 在“分发可用于此产品列表的更新”选项组中单击“添加”按钮选择要添加的产品，在“选择产品组件”选项组中选择要添加的组件，在“选择调度”选项组中选择计划的执行频率。
- ③ 单击“确定”按钮，添加完成一个分发调度，如图 20-65 所示。

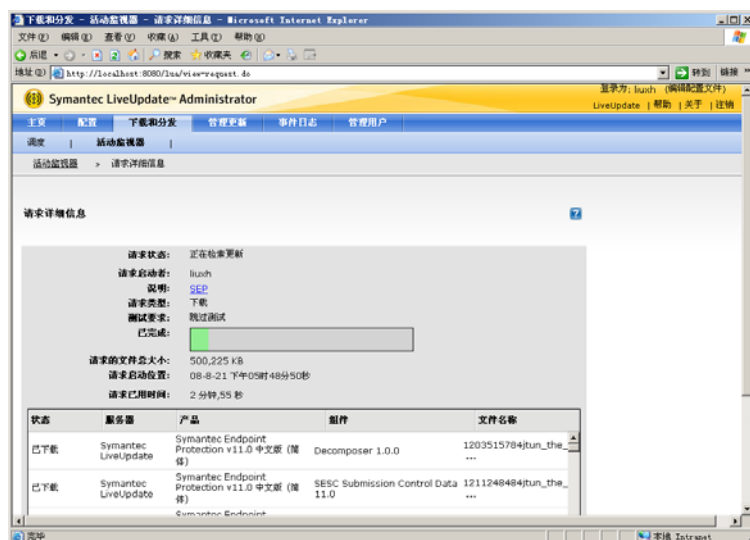


图 20-63 正在下载更新

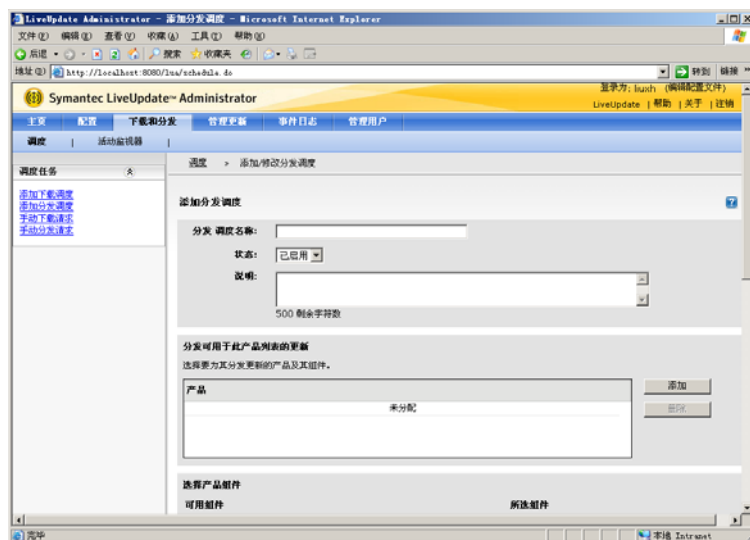


图 20-64 “添加分发调度”窗口



图 20-65 添加完成一个分发调度

“分发中心”用于向客户端分发已下载的更新，默认情况下，LiveUpdate 创建两个分发中心。即生产和测试分发中心，并且均没有添加任何产品。如果要向客户端分发，必须首先向分发中心添加更新；否则不能分发。

分发更新的操作步骤如下。

① 在“配置”窗口中打开“分发中心”窗口，如图 20-66 所示。在其中设置分发中心的地址，默认已经创建产品和测试分发中心。当客户端需要更新时，需要从该分发中心下载更新程序。

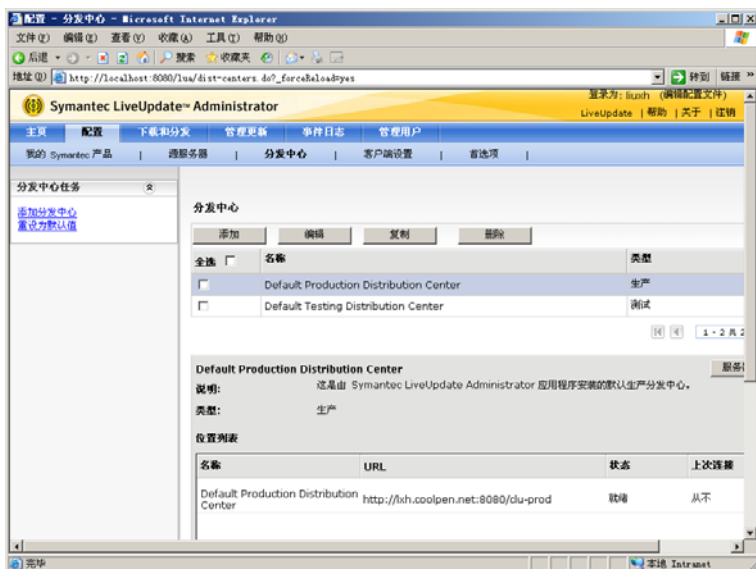


图 20-66 “分发中心”窗口

② 选择“Default Production Distribution Center”复选框，单击“编辑”按钮，显示如图 20-67 所示的“添加产品”窗口，在“所有产品”选项组中选择要添加到分发中心的 Symantec 产品。

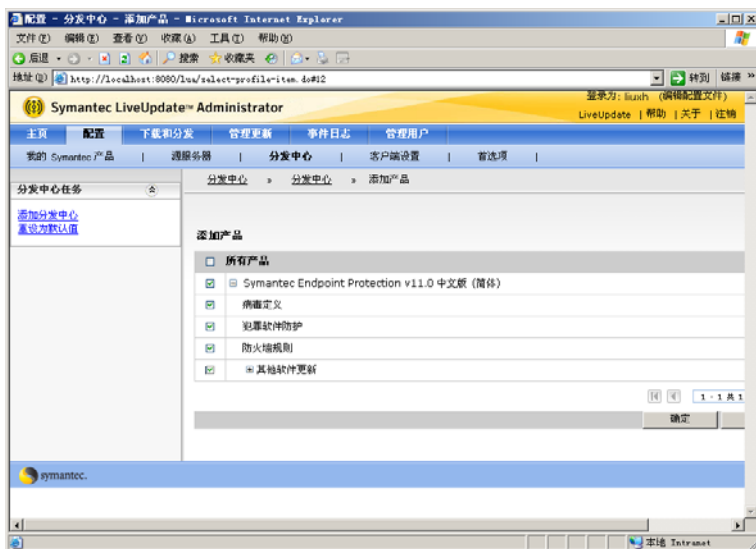


图 20-67 “添加产品”窗口

提示

如果未添加产品，则无法向客户端分发更新。

③ 单击“确定”按钮，返回“分发中心”窗口，添加完成产品。单击“确定”按钮保存即可，此时可以向客户端分发更新。

④ 打开“下载和分发”窗口，选择已创建的分发调度。单击“立即运行”按钮，开始向客户端

分发更新，如图 20-68 所示。

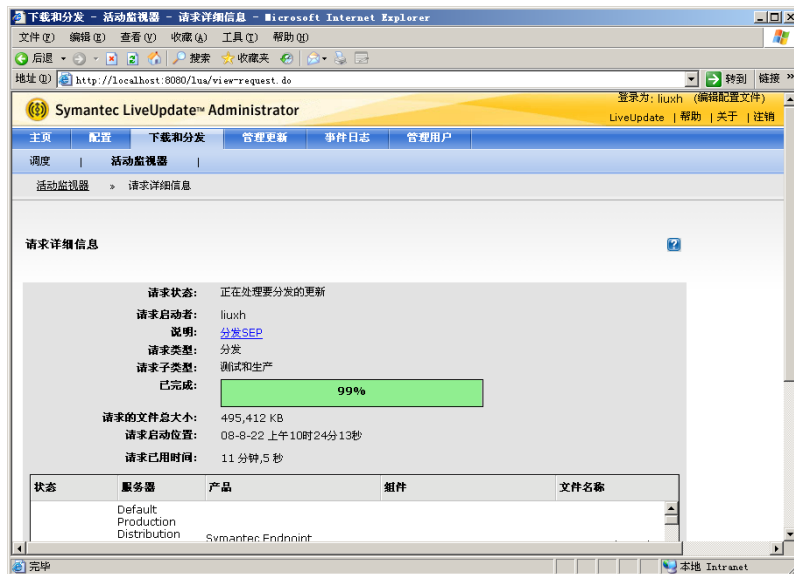


图 20-68 分发更新

⑤ 分发完成后单击“确定”按钮。

20.3.3 配置 LiveUpdate 策略

默认状态下，客户端 Symantec Endpoint 升级时从 Symantec 网站下载更新。为了使客户端在升级时可以自动从 LiveUpdate 服务器上下载，需要配置 LiveUpdate 策略。

① 登录到“Symantec Endpoint Protection Manager 控制台”，单击“策略”按钮，显示如图 20-69 所示的策略控制台。

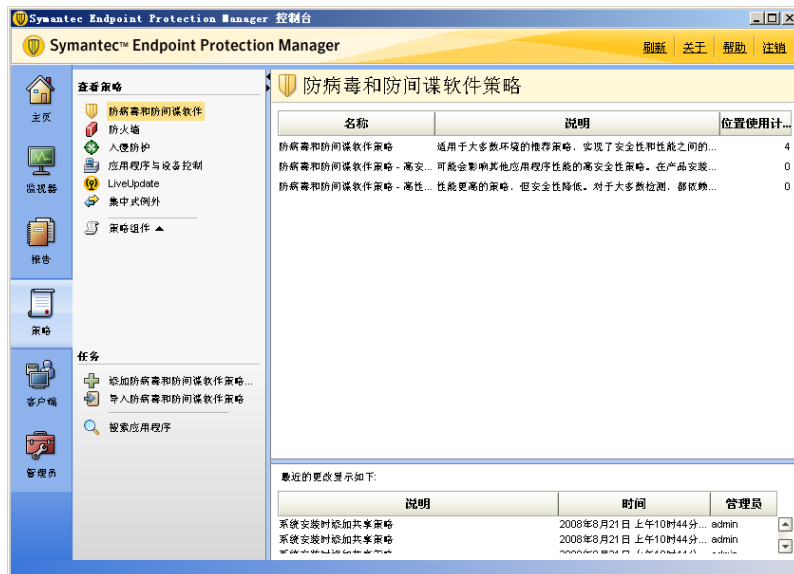


图 20-69 策略控制台

② 在左窗格的“查看策略”栏中选择“LiveUpdate”选项，显示如图 20-70 所示的“LiveUpdate 策略”窗口。

③ 选择“LiveUpdate 设置策略”选项，右击并选择快捷菜单中的“编辑”选项，显示如图 20-71 所示的“LiveUpdate 策略”对话框。

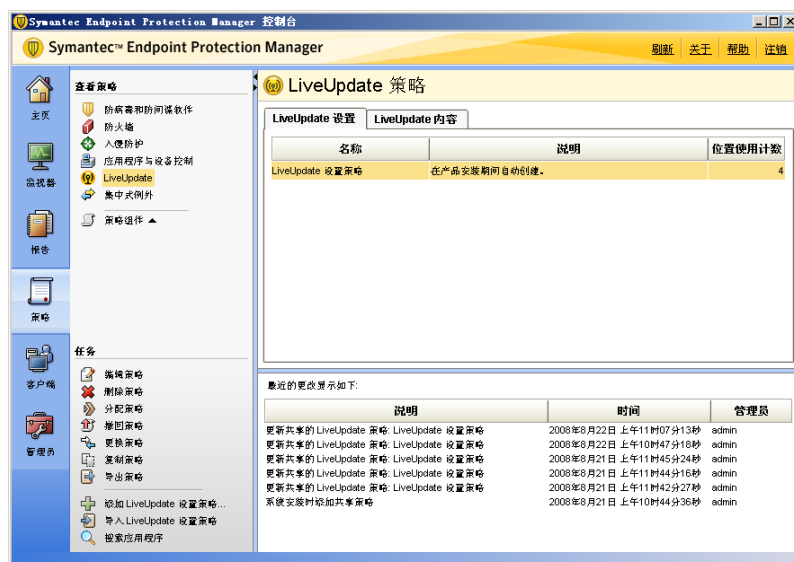


图 20-70 “LiveUpdate 策略”窗口



图 20-71 “LiveUpdate 策略”对话框

④ 在左窗格中单击“服务器设置”选项，显示如图 20-72 所示的“服务器设置”对话框，选择“使用 LiveUpdate 服务器”复选框和“使用指定的内部 LiveUpdate 服务器”单选按钮。

⑤ 单击“添加”按钮，显示如图 20-73 所示的“添加 LiveUpdate 服务器”对话框。在“服务器名”文本框中输入 LiveUpdate 服务器的计算机名。在“URL”文本框中键入 URL，格式为“http://LiveUpdate 服务器名:8080”，例如 http://lxh.coolpen.net:8080。在“用户名”和“密码”文本框中输入 LiveUpdate 服务器的用户名和密码。

⑥ 单击“确定”按钮添加成功，如图 20-74 所示。如果需要更改，则单击“编辑”按钮。

⑦ 单击“确定”按钮，LiveUpdate 策略设置完成。

这样在客户端运行 LiveUpdate 时就会自动连接 LiveUpdate 服务器并下载更新。

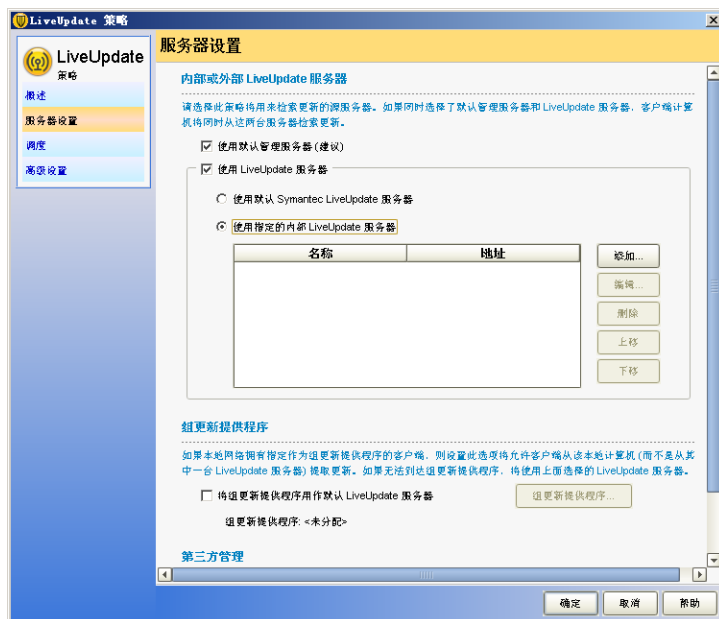


图 20-72 “服务器设置”对话框



图 20-73 “添加 LiveUpdate 服务器”对话框

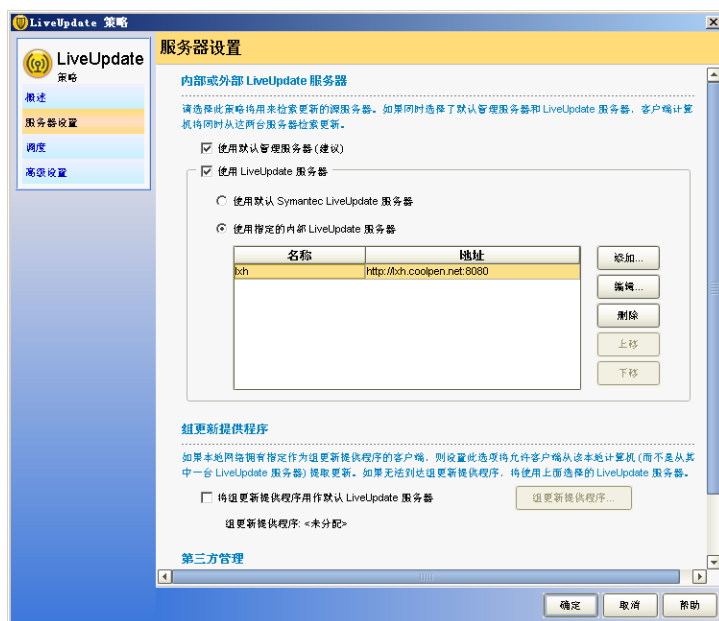


图 20-74 成功添加 LiveUpdate 服务器

第 21 章 流媒体服务

随着宽带入户的不断普及和网络带宽的不断提升，视频点播、播客等技术的流行，使得传统的文字和图片浏览已不能满足人们的需求，人们更喜欢在网上看电影、听音乐。而视频点播功能的实现，就需要利用流媒体服务器来实现。微软公司提供了 Windows Media 服务，可以用来搭建流媒体服务器，为网络提供流媒体文件在线播放。

21.1 流媒体服务的安装

通常情况下，用户需要将多媒体文件下载到计算机上才能播放，但由于多媒体文件通常比较大，所以，完全下载到本地往往需要较长时间。而利用流媒体服务，可以一边下载一边播放，无需长时间的等待。Windows Media 服务支持微软所有格式的多媒体文件，而且是免费的，可用来搭建流媒体服务。

►► 21.1.1 流媒体概述

实现流媒体技术用到的是流式媒体文件。流是用于描述媒体文件的词，在网络上称之为“流媒体”技术。流是一种传输方式，使用以 .asf、.wma、.wmv 为扩展名的流文件进行传输。用流的方式传输数据时，传输速度是不变的，用户可以一边下载一边播放，而不必像传统文件那样必须等到文件完全下载之后才能调用相应的应用程序打开。例如，流好比在水管中流动的水，水从水管口不断地流出，而水管里面的水还在不断地向前流动，流即是如此：在第一部分数据开始播放的同时，数据的其余部分源源不断地流出，及时到达目的地以供播放。流的使用，使得每个客户端在通过网络接收内容，可以边接收边欣赏，而无需首先下载该内容，不必再经过漫长且难以忍受的等待时间。流不仅大大减少了客户端的等待时间和存储需求，同时也允许无限长度的演示及实况转播。

Windows Media 服务可以发布多种 Windows 支持的流媒体格式，包括 WMA、WMV、ASF、WAV、MP3 等多种流格式，客户端用户使用 Windows 系统自带的 Windows Media Player 即可播放。而要得到这些流格式文件，除了从网上下载或者购买相应的多媒体文件以外，还可以使用 Media 编码器，将普通的多媒体文件或者实况信息转换成流媒体格式。

►► 21.1.2 流媒体传输协议

Windows Media 服务支持的流媒体传输协议主要有两种：MMS 协议（微软媒体服务协议）和 HTTP 协议。

1. MMS 协议

MMS 是微软的专有流式媒体协议，Windows Media 服务器使用该协议向客户端传输流文件。使用 MMS 协议时，播放器可以实现流文件的播放、暂停、停止、快进、倒退和索引数字媒体文件等功能。MMS 协议传输的文件可以使用 Windows Media Player 播放来播放。

MMS 协议支持微软的流媒体文件格式，也就是 Windows Media Player 所支持的文件格式，包括 AVI、MP3、WMA、WMV、ASF 等。

2. HTTP

流媒体服务也可以使用 HTTP 实现。由于 HTTP 可以通过路由器和防火墙，因此，无论用户处在

局域网还是 Internet 中，都可以使用 HTTP 穿过防火墙连接到流媒体服务器。

HTTP 可以支持 MMS 和 RTSP 协议所支持的所有文件格式。但是，当使用 HTTP 协议传输文件时，客户端也可以使用网际快车、迅雷等下载软件利用多线程直接下载文件。不过这样会占用大量的带宽，因此不建议普通用户使用 HTTP。

21.1.3 点播与广播

Windows Media 服务发布流文件通常有两种方式，即点播与广播。

点播是指用户主动向流媒体服务器发出请求并接收流文件。客户端以点播方式播放流文件时，可以对流文件进行自由控制，例如开始、停止、后退、快进或暂停等。但这种方式对带宽和服务器的要求较高，会消耗大量的网络带宽和系统资源。因此，通常只适合于在局域网内使用，或者在举行技术培训、产品发布、重要会议新闻等活动时使用。

广播是指由服务器主动发送流文件，用户被动接收。当客户端以广播方式播放服务器中的流文件时，只能接收而不能控制，例如，用户不能暂停、快进或后退，就像看电视一样，无法控制频道节目的进程。不过，广播方式对带宽占用较少，比较节省网络带宽和服务器资源。当向 Internet 提供视频点播，或者播放会议、新闻事件时，可以采用广播方式。

21.1.4 Windows Media 服务的安装

虽然 Windows Media 服务是微软公司的服务组件，但在 Windows Server 2008 系统中并没有集成，用户需要从微软网站免费下载 Windows Media Services 2008 程序，或者在系统自动下载更新时选择安装，该 Windows 更新程序代码为 KB934518。

① 运行 Windows 更新程序 (KB934518)，显示如图 21-1 所示的“Windows 更新独立安装程序”对话框。



图 21-1 Windows 更新程序

② 单击“确定”按钮，显示如图 21-2 所示的“阅读这些许可条款”对话框。

③ 单击“我接受”按钮，开始安装该更新程序。安装完成后，显示如图 21-3 所示的对话框，提示安装完成。单击“关闭”按钮关闭即可。



图 21-2 “阅读这些许可条款”对话框

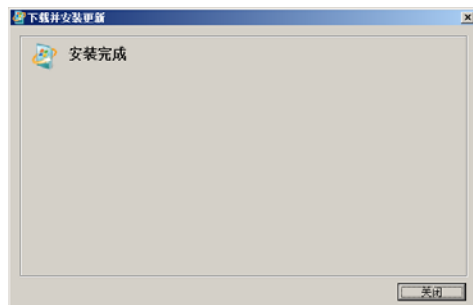


图 21-3 安装完成

④ 打开“服务器管理器”，运行“添加角色向导”，当显示“选择服务器角色”对话框时，在“角色”列表中即可看到“流媒体服务”，如图 21-4 所示，选中该复选框即可。

⑤ 单击“下一步”按钮，显示如图 21-5 所示“流媒体服务”对话框，简要介绍了流媒体服务的概述信息。

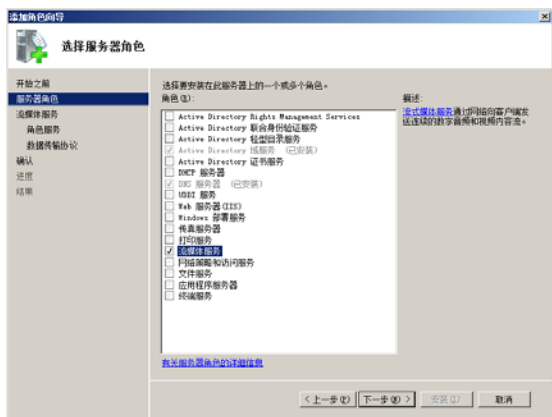


图 21-4 “选择服务器角色”对话框



图 21-5 “流媒体服务”对话框

⑥ 单击“下一步”按钮，显示如图 21-6 所示“选择角色服务”对话框，用来选择流媒体服务的组件。

⑦ 单击“下一步”按钮，显示如图 21-7 所示“选择数据传输协议”对话框，用来选择流媒体数使用用的传输协议。如果要为运行 Windows Media Player 9 或更高版本的客户端提供流媒体服务，应选中“实时流协议 (RTSP)”复选框，如果要为运行任何版本客户端提供，则应选中“超文本传输协议 (HTTP)”复选框。

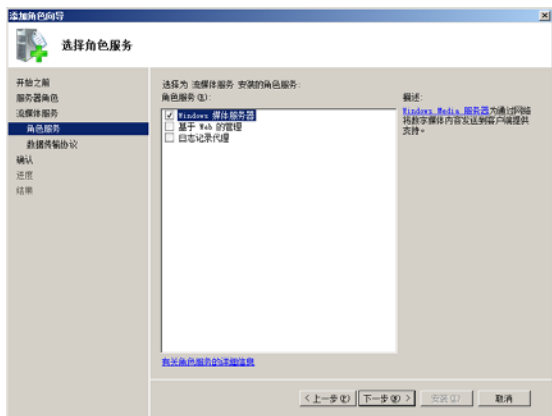


图 21-6 “选择角色服务”对话框

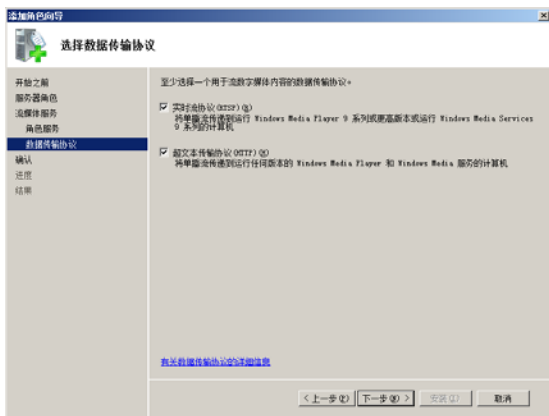


图 21-7 “选择数据传输协议”对话框

⑧ 单击“下一步”按钮，显示如图 21-8 所示“确认安装选择”对话框，列出了将要安装的服务。

⑨ 单击“安装”按钮，开始安装流媒体服务。安装完成后，显示如图 21-9 所示“安装结果”对话框。



图 21-8 “确认安装选择”对话框

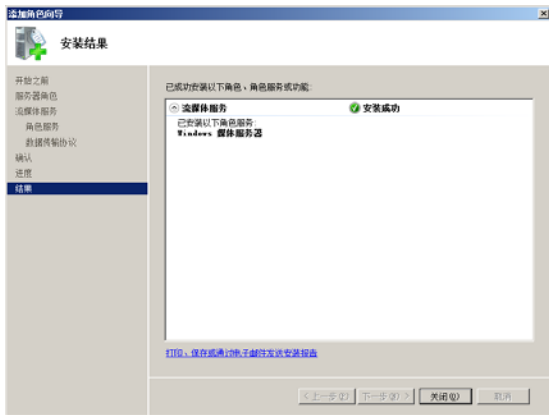


图 21-9 “安装结果”对话框

⑩ 单击“关闭”按钮，流媒体服务安装完成。

依次单击“开始”→“管理工具”→“Windows Media 服务”，显示如图 21-10 所示的“Windows Media 服务”窗口，现在就可以配置 Windows Media 服务了。

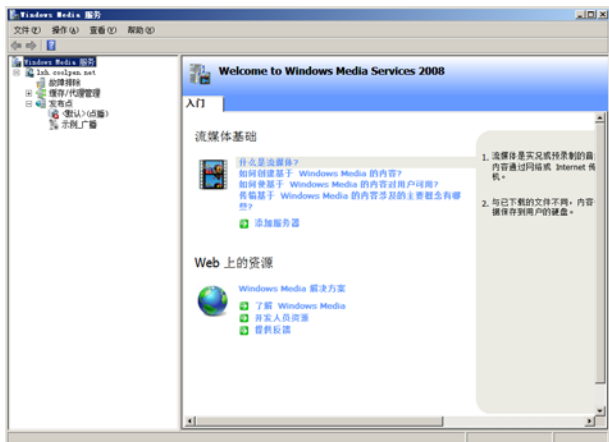


图 21-10 “Windows Media 服务”窗口

21.2 实现点播和广播

由于带宽限制、访问授权、缓存启用等有关访问安全和服务性能的限置，只能对不同的点播发布点分别设置，因此，有时需要创建多个发布点，以适应不同用户的访问和不同流媒体文件发布的需要。创建发布点可以使用向导和高级两种方法。

21.2.1 实现视频和音频点播

默认情况下，Windows 已经创建了一个默认点播和广播发布点。在“Windows Media 服务”窗口中，展开“发布点”，即可看到已创建的点播和广播发布点，如图 21-11 所示。用户也可以另行创建新的点播和广播发布点，并且分别可以使用向导和高级方法创建。

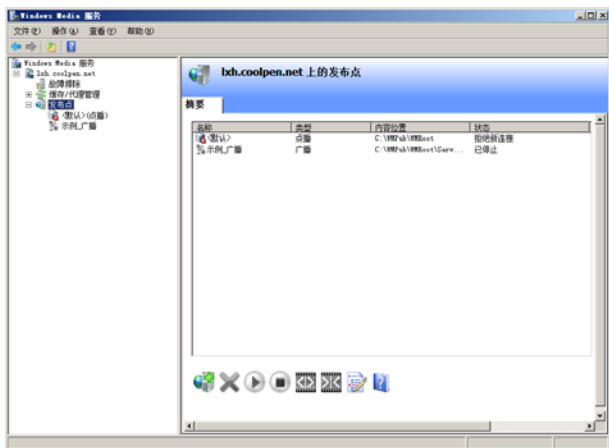


图 21-11 发布点

这里以向导方式创建点播发布点为例，将服务器中的视频文件创建为点播发布点。

① 右击“发布点”，选择快捷菜单中的“添加发布点（向导）”选项，运行“添加发布点向导”，如图 21-12 所示。

② 单击“下一步”按钮，显示如图 21-13 所示“发布点名称”对话框，在“名称”文本框中可设置该发布点的名称，默认为“PublishingPoint1”。



图 21-12 添加发布点向导

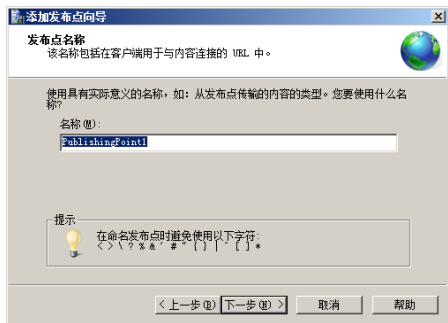


图 21-13 “发布点名称”对话框

③ 单击“下一步”按钮，显示如图 21-14 所示“内容类型”对话框，列出了 4 种要传输的内容的类型以供选择：

编码器（实况流）：将从麦克风、摄像头等设备捕获的实况流编码成流文件并进行广播。由于内容不是 Windows Media 文件，所以，通常将它称为实况流。不过，仅适用于广播发布点，所以在建立点播时不能选择该项。

播放列表：可以创建一个具有一个或多个文件的列表，将该系列流文件通过播放列表播放。

一个文件：使用发布点传输单个文件。

目录中的文件：指定要添加到视频点播的文件夹。这里选择该项，在该点播发布点中发布目录中的流文件。

④ 单击“下一步”按钮，显示如图 21-15 所示“发布点类型”对话框，选择“点播发布点”，创建点播发布点。

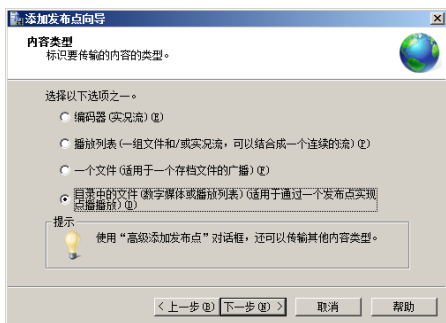


图 21-14 “内容类型”对话框

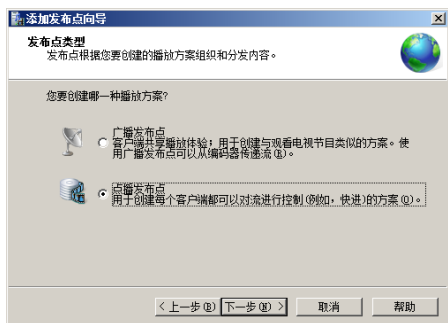


图 21-15 “发布点类型”对话框

⑤ 单击“下一步”按钮，显示如图 21-16 所示的“目录位置”对话框，单击“浏览”按钮，选择流文件所在的文件夹。

⑥ 单击“下一步”按钮，显示如图 21-17 所示的“内容播放”对话框，设置目录中文件的播放顺序，可以是循环播放或无序播放。

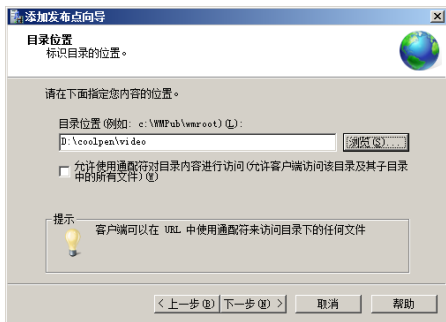


图 21-16 “目录位置”对话框

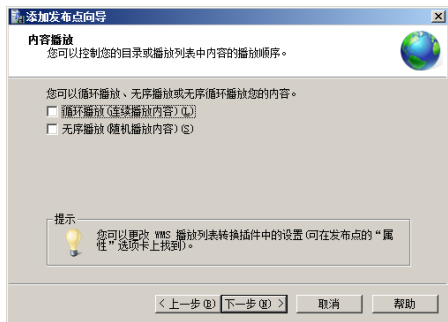


图 21-17 “内容播放”对话框

⑦ 单击“下一步”按钮，显示如图 21-18 所示的“单播日志记录”对话框。选中“是，启用该发布点的日志记录”复选框，可启用单播日志记录，从而便于查看哪些节目最受欢迎、每天哪段时间服务器最忙碌等信息，并据此对内容和服务进行调整。

⑧ 单击“下一步”按钮，显示如图 21-19 所示的“发布点摘要”对话框，列出了前面所做的配置。

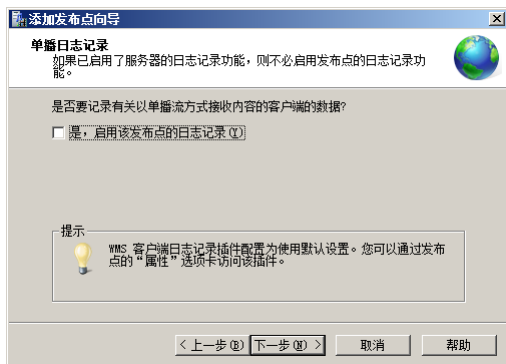


图 21-18 “单播日志记录”对话框

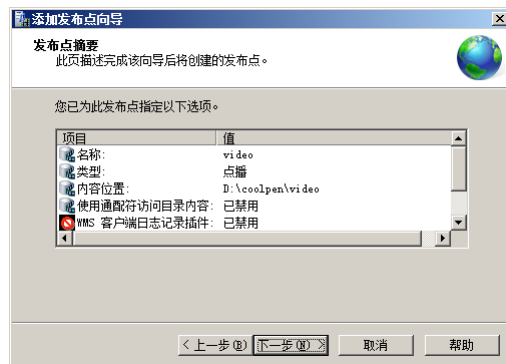


图 21-19 “发布点摘要”对话框

⑨ 单击“下一步”按钮，显示如图 21-20 所示的“正在完成‘添加发布点向导’”对话框，选中“完成向导后”复选框，并选择“创建公告文件 (.asx) 或网页 (.htm)”单选按钮，来创建一个点播公告文件。

创建公告文件 (.asx) 或网页 (.htm)：启动公告向导来引导用户完成创建公告的过程。也可以在发布点“公告”选项卡中随时启动公告向导。

创建包装播放列表 (.wsx)：启动“创建包装向导”来帮助用户创建内容的包装播放列表。也可以通过单击发布点“广告”选项卡上的“包装编辑器”按钮随时启动“创建包装向导”。

创建包装播放列表 (.wsx) 以及公告文件 (.asx) 或网页 (.htm)：将按顺序启动“创建包装向导”和相应的公告向导。

⑩ 单击“完成”按钮，运行“单播公告向导”，如图 21-21 所示。

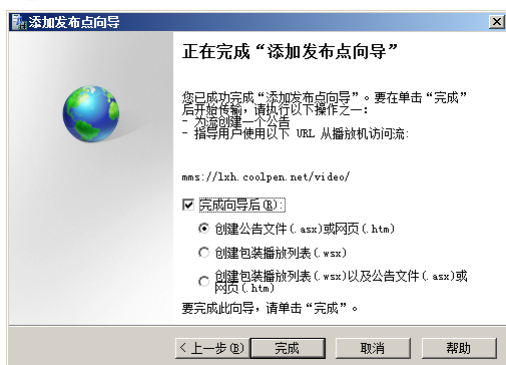


图 21-20 完成添加发布点向导



图 21-21 单播公告向导

⑪ 单击“下一步”按钮，显示如图 21-22 所示的“点播目录”对话框，在“目录中的一个文件”文本框中键入要发布的流媒体文件路径，或者单击“浏览”按钮选择。

⑫ 单击“下一步”按钮，显示如图 21-23 所示的“访问该内容”对话框。默认以“mms://计算机名/目录名/文件名”的格式发布点播文件。

如果要以 IP 地址或域名的文件发布 URL 地址，可单击“修改”按钮，显示如图 21-24 所示“修改服务器名称”对话框。在“名称”文本框中键入该视频服务器的 IP 地址或域名，单击“确定”按钮即可。

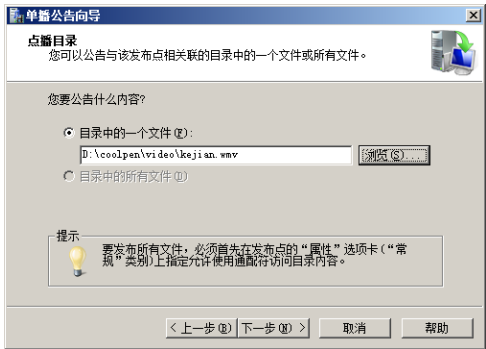


图 21-22 “点播目录”对话框

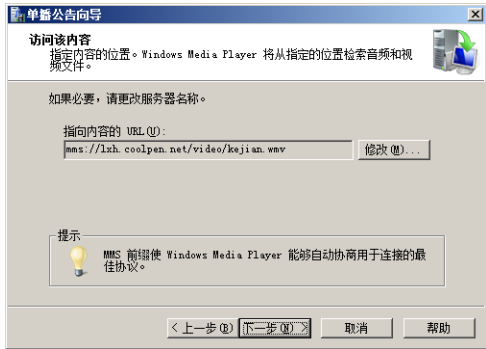


图 21-23 “访问该内容”对话框

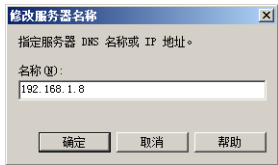


图 21-24 “修改服务器名称”对话框

⑬ 单击“下一步”按钮，显示如图 21-25 所示的“保存公告选项”对话框，选中“创建一个带有嵌入的播放机和指向该内容的链接的网页”复选框，并指定保存该公告和网页文件的名称和位置。

⑭ 单击“下一步”按钮，显示“编辑公告元数据”对话框，设置公告文件的标题、作者、版权等等信息，如图 21-26 所示。这些信息将在用户接收内容时出现在 Windows Media Player 的标题区域。

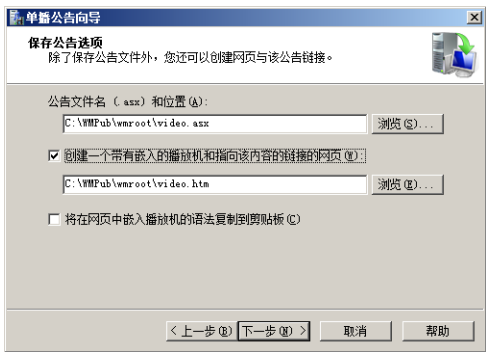


图 21-25 “保存公告选项”对话框

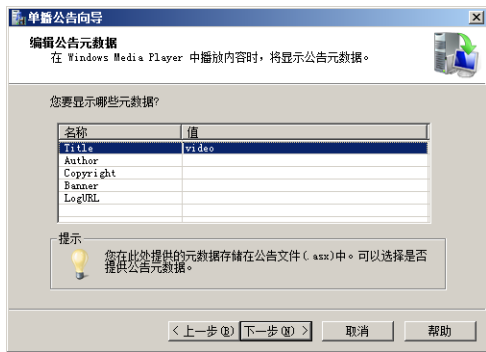


图 21-26 “编辑公告元数据”对话框

⑮ 单击“下一步”按钮，显示如图 21-27 所示“正在完成‘单播公告向导’”对话框，选中“完成此向导后测试文件”复选框。

⑯ 单击“完成”按钮，显示如图 21-28 所示“测试单播公告”对话框。

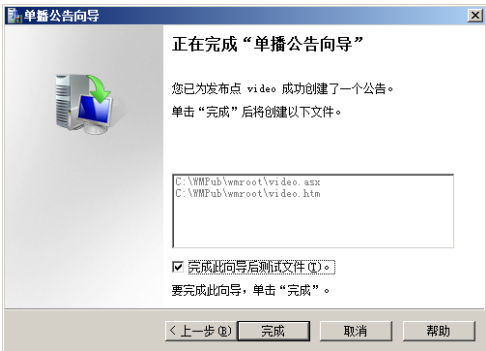


图 21-27 正在完成“单播公告向导”

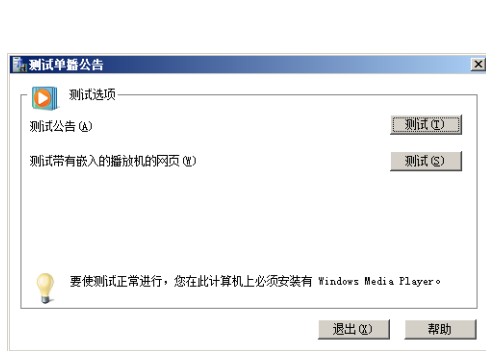


图 21-28 “测试单播公告”对话框

⑪ 单击“测试”按钮，可以分别测试公告和网页是否正确，是否能够正常播放流文件。不过，Windows Server 2008 系统中没有安装 Windows Media Player，因此，无法播放，如图 21-29 所示，可在网络中的其他计算机进行测试。

如果用户已经熟悉了发布点的创建过程，也可以使用高级方式来创建发布点。在“Windows Media 服务”窗口中，右击“发布点”并选择快捷菜单中的“添加发布点（高级）”选项，显示如图 21-30 所示“添加发布点”对话框。在“发布点类型”选项区域中选择“点播”单选按钮，在“发布点名称”文本框中为该发布点设置一个名称，“内容的位置”文本框中键入流文件所在的路径，单击“确定”按钮即可。

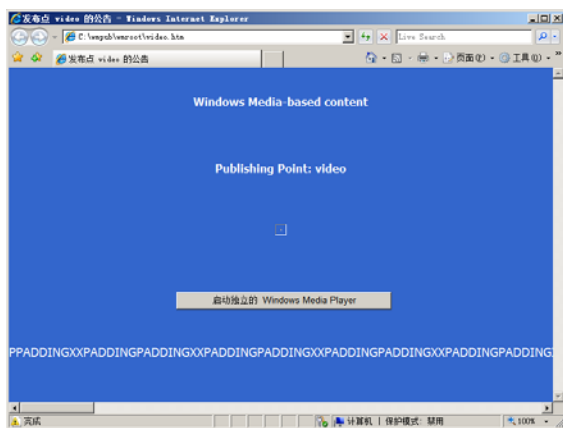


图 21-29 测试公告

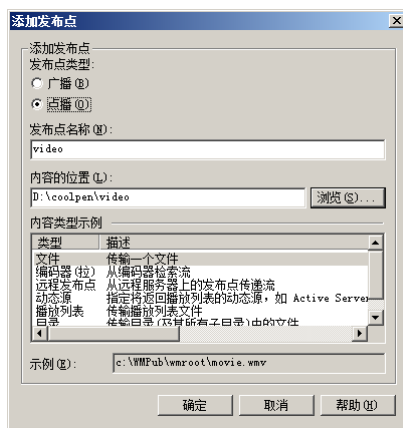


图 21-30 “添加发布点”对话框

21.2.2 实现视频和音频广播

创建视频和音频广播的方式和创建点播点类似，都可以通过“添加发布点向导”来完成，并可分别通过向导和高级方式来创建。

① 在“Windows Media 服务”窗口中，展开左侧树型目录，右击“发布点”并在快捷菜单中的选择“添加发布点（向导）”选项，运行“添加发布点向导”。

② 单击“下一步”按钮，显示如图 21-31 所示的“发布点名称”对话框，在“名称”文本框中键入该发布点的名称。

③ 单击“下一步”按钮，显示如图 21-32 所示的“内容类型”对话框，选择欲广播的内容类型，可以选择使用播放列表，或者使用文件。

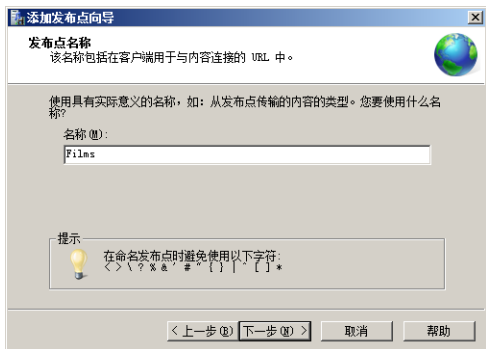


图 21-31 “发布点名称”对话框

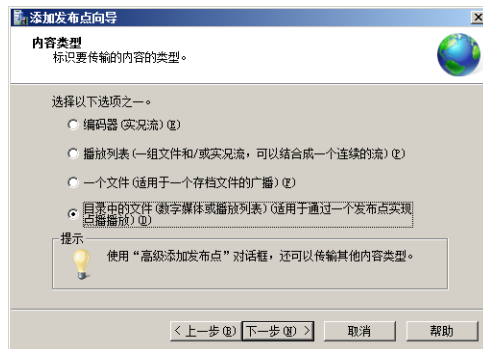


图 21-32 “内容类型”对话框

④ 选择“播放列表”单选按钮，单击“下一步”按钮，显示如图 21-33 所示的“发布点类型”对话框，选择“广播发布点”单选按钮。

⑤ 单击“下一步”按钮，显示如图 21-34 所示的“广播发布点的传递选项”对话框，选择“单播”单选按钮。

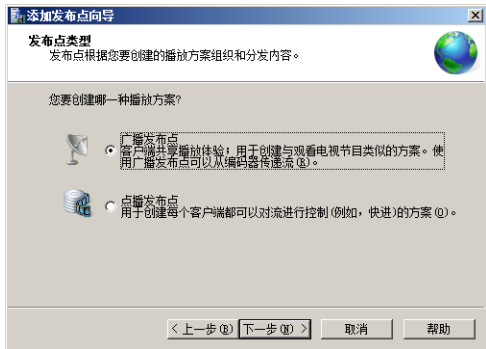


图 21-33 “发布点类型”对话框

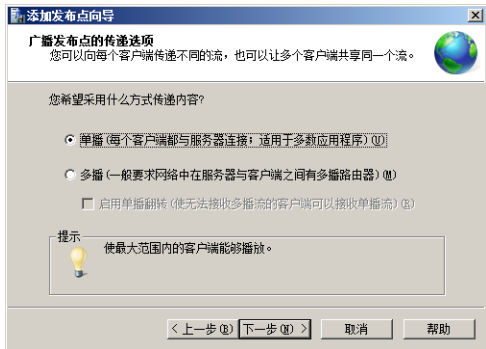


图 21-34 “广播发布点的传递选项”对话框

⑥ 单击“下一步”按钮，显示如图 21-35 所示“目录位置”对话框，在“目录位置”文本框中键入视频和音频文件夹的路径，或者单击“浏览”按钮选择。

⑦ 继续单击“下一步”按钮，后面的操作与创建点播发布点时完成相同，这里不再赘述。

和创建点播发布点一样，也可以使用高级方法创建广播发布点。在 Windows Media Services 窗口中右击“发布点”，选择快捷菜单中的“添加发布点（高级）”选项，显示如图 21-36 所示对话框。选择“广播”单选按钮，在“发布点名称”文本框中键入名称，单击“浏览”按钮选择流媒体文件，单击“确定”按钮即可。

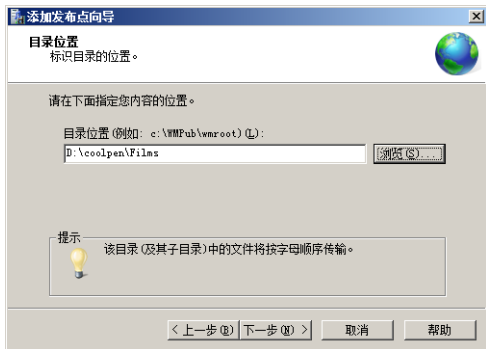


图 21-35 “文件位置”对话框

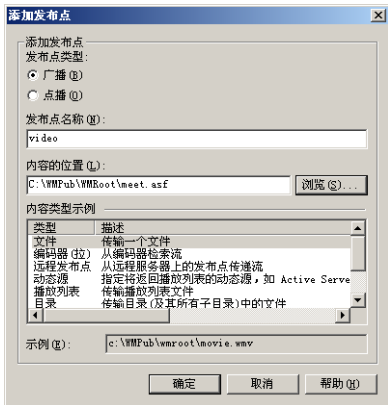


图 21-36 “添加发布点”对话框

21.2.3 制作播放列表

如果欲发布多个多媒体文件，就可以采用播放列表来实现。这样就可以将多个流媒体文件制作成一个播放列表，例如添加专辑等，这样，当用户在点播该播放列表时就可以自动连续播放多个文件，而不必逐个点播。播放列表可以在创建广播和点播发布点时创建，也可以在某个发布点中另行创建，即可利用播放列表来代替欲发布的文件。

① 在“Windows Media 服务”窗口中，选择欲创建播放列表的发布点，在右侧窗口中选择“源”选项卡，如图 21-37 所示。

② 单击“查看播放列表编辑器”图标，显示如图 21-38 所示“播放列表”对话框。选择“新建一个新的播放列表”单选按钮，创建一个新的播放列表。

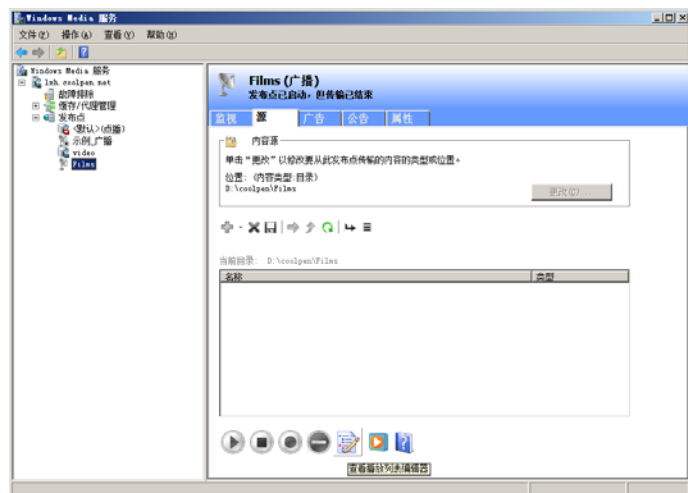


图 21-37 “源”选项卡

- ③ 单击“确定”按钮，显示如图 21-39 所示“Windows Media 播放列表编辑器”窗口。

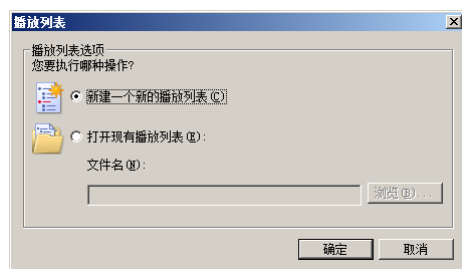


图 21-38 “播放列表”对话框

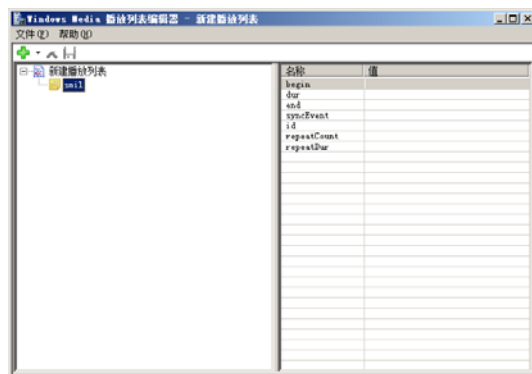


图 21-39 Windows Media 播放列表编辑器

- ④ 在“新建播放列表”目录中右击“smil”，选择快捷菜单中的“添加媒体”选项，显示如图 21-40 所示“添加媒体元素”对话框，单击“浏览”按钮选择欲制作播放列表的文件夹或文件，可以是单个文件或文件夹，也可以同时选择多个文件。

- ⑤ 单击“确定”按钮，返回“Windows Media 播放列表编辑器”窗口，如图 21-41 所示，列出了添加至该播放列表的文件目录。

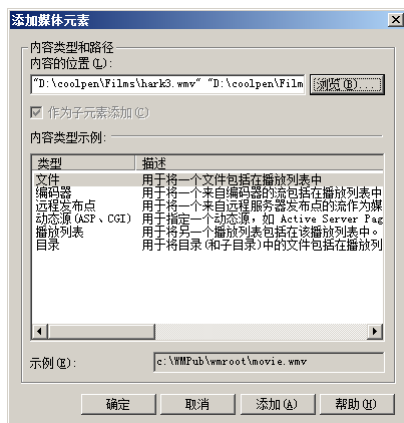


图 21-40 “添加媒体元素”对话框

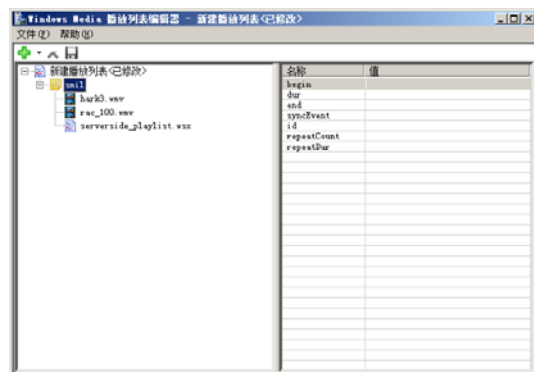


图 21-41 添加至播放列表的多媒体文件

- ⑥ 单击“保存”按钮，将该播放列表保存即可。

然后,再制作一个 Web 网页,为该播放列表添加超级列表,当用户单击该超级链接时,即可播放该播放列表中的文件。

21.2.4 发布广告

广告是使用最多的宣传方式之一,在流媒体服务器也可以设置广告。当用户设置播放列表时,即可在多媒体文件中插播广告,使用户在播放流媒体文件的过程中,可自动播放广告文件。插播广告的制作与播放列表的制作基本相同,不过,在插播广告时可以调整节目的播放顺序。

若在播放列表中插入广告,可在“Windows Media 播放列表编辑器”窗口中右击“smil”,选择快捷菜单中的“添加广告”选项,显示如图 21-42 所示“添加广告”对话框。单击“浏览”按钮选择广告文件,单击“确定”按钮即可添加广告。



图 21-42 “添加广告”对话框

如果要在发布点中直接添加广告,可执行如下操作步骤:

① 在“Windows Media Services”控制台窗口中选择欲创建播放列表的该点播发布点,并在右侧栏中选择“广告”选项卡,如图 21-43 所示。

② 单击位于窗口底端的“包装编辑器”图标,显示如图 21-44 所示的“包装播放列表编辑器选项”对话框。选择“创建播放列表文件”单选按钮,并选中“使用创建包装向导”复选框,启用创建包装向导制作包含有广告内容的播放列表。

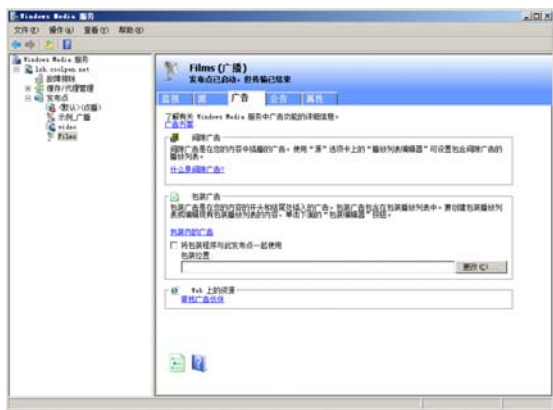


图 21-43 “广告”选项卡

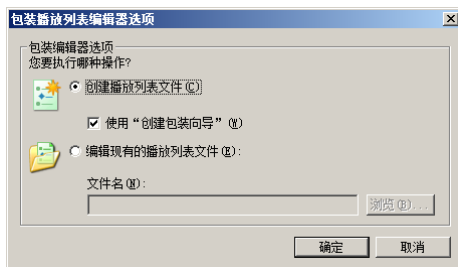


图 21-44 包装播放列表编辑器选项

③ 单击“确定”按钮,显示如图 21-45 所示“创建包装向导”。

④ 单击“下一步”按钮,显示如图 21-46 所示“包装播放列表文件”对话框,可以在客户端请求的内容之前或之后插入文件。

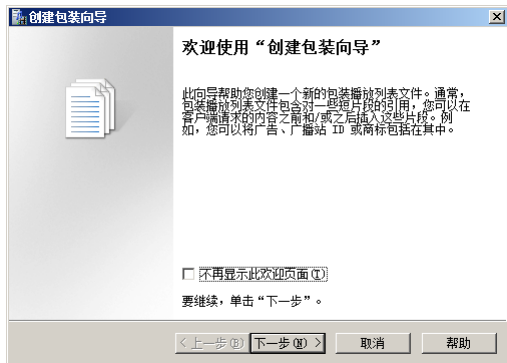


图 21-45 创建包装向导



图 21-46 “包装播放列表文件”对话框

⑤ 单击“添加媒体”按钮，显示如图 21-47 所示“添加媒体元素”对话框，单击“浏览”按钮，添加查找并选择欲添加播放列表的流媒体文件或文件夹。单击“确定”按钮返回。

⑥ 单击“添加广告”按钮，显示如图 21-48 所示“添加广告”对话框。在文本框中键入广告文件的文件名及其文件夹，单击“确定”按钮。重复操作，可添加多条广告。

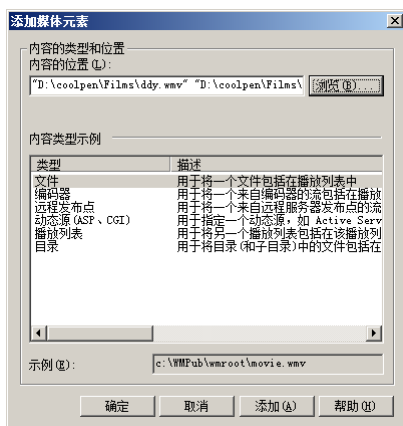


图 21-47 “添加媒体元素”对话框



图 21-48 “添加广告”对话框

⑦ 流媒体文件和广告添加完成后，在列表框中可以调整媒体的播放顺序。选择欲调整顺序的文档，单击“上移”、“下移”按钮，即可上下移动其位置。

⑧ 单击“下一步”按钮，显示如图 21-49 所示“保存包装播放列表文件”对话框，键入该播放列表保存路径及文件名。

⑨ 单击“下一步”按钮，显示如图 21-50 所示创建包装向导完成页。单击“完成”按钮，包含有广告的播放列表创建完成。

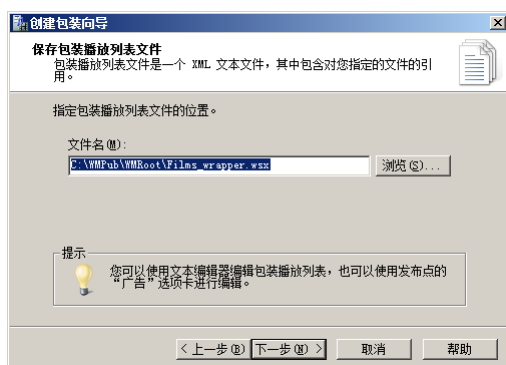


图 21-49 “保存包装播放列表文件”对话框

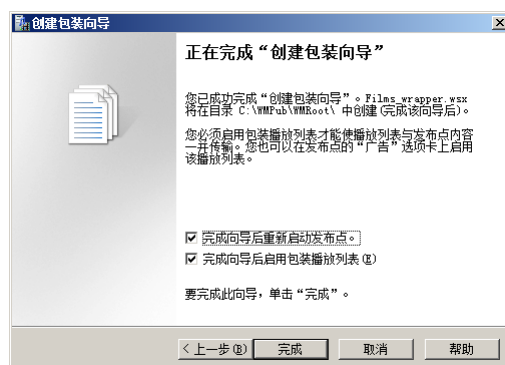


图 21-50 完成创建包装向导

21.2.5 对点播发布点的访问

对于客户端用户，可以通过上述制作的.asx 通知文件访问，或通过包含有通知文件或流文件超级链接的 HTML 文件访问点播发布点中的所有流文件。另外，用户也可以在自己的 Windows Media Player 中键入对应的 URL 地址来访问相应的流文件。

1. 使用 MMS 协议访问

当流文件位于 Home 点播发布点（即默认点播发布点）根目录时，利用 Windows Media Player 访问时，需键入下述 URL：

```
mms://Media 服务器 IP 地址/流媒体文件名或播放列表名
mms://Media 服务器域名/流媒体文件名或播放列表名
```

当流文件位于点播发布点中的某个子目录时，利用 Windows Media Player 访问时，需键入下述

URL:

```
mms://Media 服务器 IP 地址/子目录/流媒体文件名或播放列表名
```

```
mms://Media 服务器域名/子目录/流媒体文件名或播放列表名
```

如果流文件位于非 Home 点播发布点时，利用 Windows Media Player 访问时，需键入下述 URL:

```
mms://Media 服务器 IP 地址/别名/流媒体文件名或播放列表名
```

```
mms://Media 服务器域名/别名/流媒体文件名或播放列表名
```

2. 用 Web 服务器传送流文件

除了用 Windows Media 服务传送流文件外，也可以使用 Web 服务器来传送流式内容。只要将流文件放置到 Web 目录中，并在 Web 页中为它们创建一个超级链接，然后，客户端点击相应的超级链接时，即可使用 HTTP 协议将内容以流的格式传送给用户。在这种情况下，流传送由 Web 服务器所管理，因此，可以不必安装 Windows Media 服务。但是，使用 Web 方式传输流方式，占用的带宽较大，而不具有纠正流错误的同样能力。同时，以 HTTP 方式发布的流文件也更容易被用户下载，尤其是使用迅雷等工具下载时，将占用更大的带宽，也会将流文件泄露到网络。

第 22 章 Exchange Server 2007 邮件服务

Exchange Server 2007 是目前最新的 Microsoft Exchange 产品，在 Microsoft Exchange 早期版本的基础上，增加了许多新功能，并且更安全、更灵活和可扩展性更强，为 Exchange Server 产品线带来一组丰富的新技术、功能和服务。Exchange 2007 提供不同的服务器角色，与邮件系统在组织中通常的部署和分配方式对应，旨在为各种规模的客户，提供全面、集成和灵活的邮件解决方案。使用 Exchange 2007，整个组织中的用户可以通过各种设备，在任何位置访问电子邮件、语音邮件、日历和联系人。

22.1 Exchange Server 2007 的系统需求

Exchange Server 2007 对服务器的软件和硬件都有一定的需求，尤其是需要 64 位的运行环境。这里，将在 Windows Server 2008 操作系统中部署 Exchange Server 2007。

►► 22.1.1 硬件需求

Exchange Server 2007 服务器推荐的最低硬件需求如下。

CPU：生产环境必须配备 64 位处理器，Exchange Server 2007 仅可在测试和培训环境中支持 32 位处理器。

内存：推荐为服务器配置 2 GB 的内存，以及每个邮箱 5 MB 的内存。

磁盘空间：在安装 Exchange Server 2007 的驱动器上至少具有 1.2 GB 的可用磁盘空间，对于要安装每个统一消息（UM）语言包，需要另外 500 MB 的可用磁盘空间，磁盘分区必须使用 NTFS 文件系统。

系统空间需求：系统驱动器上具有 200 MB 的可用磁盘空间，在 Exchange Server 2007 RTM（正式发布版）中，用于存储邮件队列数据库的硬盘驱动器上至少要有 4 GB 的可用空间，在 Exchange Server 2007 SP1 中，用于存储邮件队列数据库的硬盘驱动器至少要有 500 MB 的可用空间。

►► 22.1.2 软件需求

生产环境中的 Exchange Server 2007 仅支持 64 位操作系统，并且需要安装 Microsoft .NET Framework 3.0（适用于 Windows Server 2008）或 .NET Framework 2.0 组件，以及 Microsoft Windows PowerShell（适用于 Exchange 命令行管理程序）和 Microsoft 管理控制台（MMC）3.0 等。Exchange Server 2007 需要 Microsoft Active Directory 目录服务的支持，建议选择域成员服务器作为目标服务器。

Exchange Server 2007 的客户端可以是 Office Outlook 2007、Outlook 2003、Outlook 2002，也可以是安装了 Web 浏览器的计算机，运行与 Exchange ActiveSync 兼容的非 Windows 操作系统的移动设备，如手机等。

22.2 安装 Exchange Server 2007

Exchange Server 2007 需要在域环境中运行，而且需要安装 IIS 等组件。

在通常情况下，在中小型企业网络中配置一台 Exchange Server 2007 就足够了。本例中使用一台命名为 AD-Server 的计算机作为邮件服务器，首先需要将其升级为域控制器，然后再安装 Exchange Server 2007。

22.2.1 升级到 Active Directory 服务器

在安装 Exchange Server 2007 之前，需要先在服务器上打开“服务器管理器”，运行“添加角色向导”，将其升级到 Active Directory 服务器。

22.2.2 安装相关组件

在将计算机升级到 Active Directory 之后，还需要安装如下组件：

.Net Framework 2.0 或 3.0

PowerShell

MMC 3.0

IIS 7.0（根据所选角色不同会提示安装 IIS 7.0 中的不同组件）

这些组件均可在 Windows Server 2008 的“服务器管理器”窗口中安装。

① 打开“服务器管理器”窗口，单击“添加角色”按钮，显示如图 22-1 所示的“选择服务器角色”对话框，选择“Web 服务器（IIS）”复选框。同时，也选中“文件服务器”和“应用程序服务器”复选框。

② 在“添加角色向导”对话框中，单击“添加必需的功能”按钮，如图 22-2 所示。

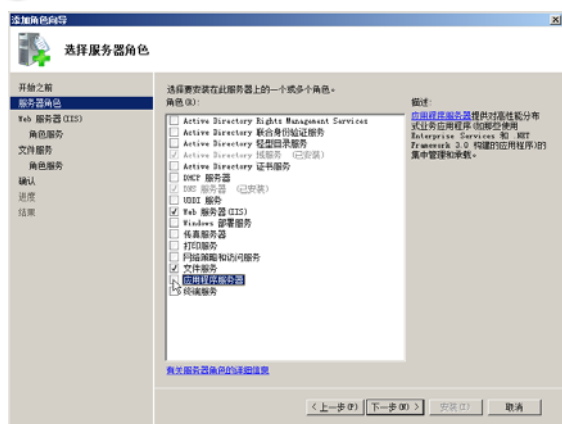


图 22-1 选择服务器角色



图 22-2 添加角色向导

③ 返回“选择服务器角色”对话框，单击“下一步”按钮，显示如图 22-3 所示的“应用程序服务器”对话框。

④ 单击“下一步”按钮，显示如图 22-4 所示“选择角色服务”对话框，选择“Web 服务器（IIS）支持”复选框。

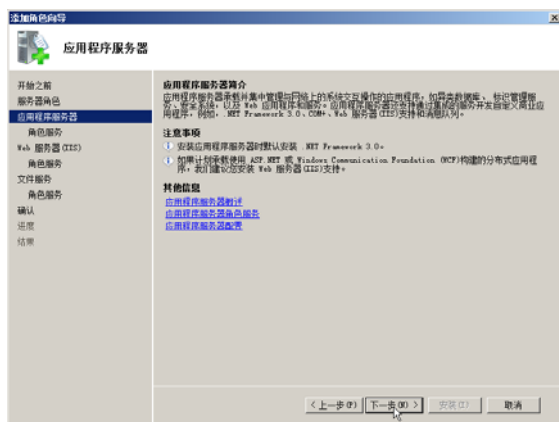


图 22-3 应用程序服务器



图 22-4 选择角色服务

⑤ 单击“下一步”按钮，显示如图 22-5 所示“Web 服务器”对话框。

⑥ 单击“下一步”按钮，显示如图 22-6 所示“选择角色服务”对话框，选中“IIS6 管理兼容性”复选框。



图 22-5 Web 服务器

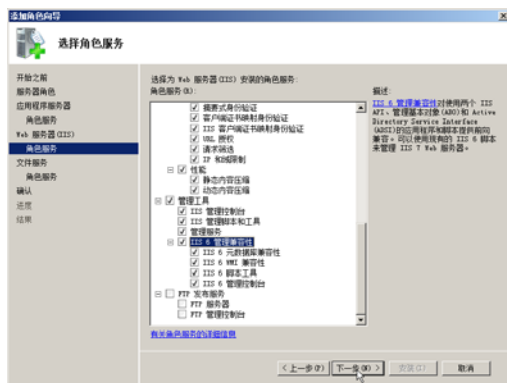


图 22-6 选择角色服务

⑦ 单击“下一步”按钮，显示如图 22-7 所示“文件服务”对话框。

⑧ 单击“下一步”按钮，显示如图 22-8 所示“选择角色服务”对话框，选择为文件服务安装的角色服务。



图 22-7 文件服务



图 22-8 选择文件服务

⑨ 单击“下一步”按钮，如图 22-9 所示“确认安装选项”对话框。

⑩ 单击“安装”按钮开始安装所选角色和组件，完成后显示如图 22-10 所示“安装结果”对话框，单击“关闭”按钮，退出安装向导即可。



图 22-9 确认安装选择



图 22-10 安装结果

⑪ 在“服务器管理器”窗口中，依次单击“功能”→“添加功能”选项，显示如图 22-11 所示“选择功能”对话框，选中“Windows PowerShell”复选框。

- ⑫ 单击“下一步”按钮，显示如图 22-12 所示“确认安装选择”对话框。



图 22-11 选择功能



图 22-12 确认安装选择

- ⑬ 单击“安装”按钮开始安装，完成后显示如图 22-13 所示的“安装结果”对话框。安装完成后，单击“关闭”按钮即可。

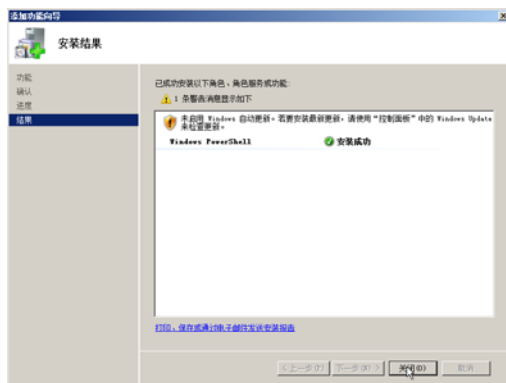


图 22-13 安装结果

22.2.3 安装 Exchange Server 2007 SP1

当必需的组件安装完成以后，就可以安装 Exchange Server 2007 了，具体的安装步骤如下。

- ① 将安装光盘插入光盘驱动器，安装程序自动运行，显示如图 22-14 所示页面，此时“安装”下的前 3 个步骤均显示“已安装”状态。
- ② 单击“步骤 4：安装 Exchange Server 2007 SP1”链接，显示如图 22-15 所示“简介”对话框，显示了关于 Exchange Server 2007 SP1 的基本信息。



图 22-14 安装界面



图 22-15 简介

- ③ 单击“下一步”按钮，显示如图 22-16 所示“许可协议”对话框，选择“我接受许可协议中的条款”单选按钮。

④ 单击“下一步”按钮，显示如图 22-17 所示“错误报告”对话框，根据需要选择是否在出现错误时向 Microsoft 公司发送报告。



图 22-16 许可协议



图 22-17 错误报告

⑤ 单击“下一步”按钮，显示如图 22-18 所示“安装类型”对话框，选择希望使用的安装方式，包括“典型安装”和“自定义安装”两种。

⑥ 单击“下一步”按钮，显示如图 22-19 所示“Exchange 组织”对话框，在“请指定此 Exchange 组织的名称”文本框中，键入 Exchange 组织名称，例如 Mail-Server。



图 22-18 安装类型



图 22-19 Exchange 组织

⑦ 单击“下一步”按钮，显示如图 22-20 所示“客户端设置”对话框，可以设置是否支持 Outlook 2003 及更早版本或 Entourage 的客户端计算机。本例中选择“是”单选按钮。

⑧ 单击“下一步”按钮，显示如图 22-21 所示“准备情况检查”对话框，安装程序将会对系统和服务器进行检查，确认是否可以安装 Exchange Server 2007。检查完成后，会自动显示检查成功和失败的项目。

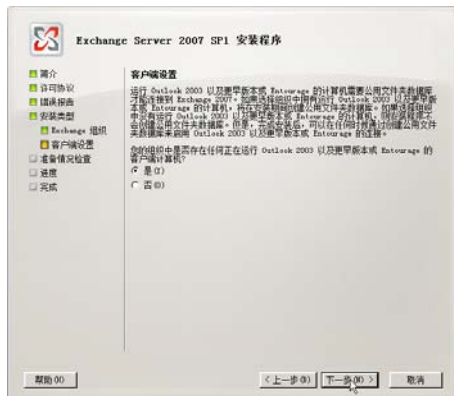


图 22-20 客户端设置



图 22-21 准备情况检查

- ⑨ 确认无误后, 单击“安装”按钮开始安装。完成后, 显示如图 22-22 所示“完成”对话框。
- ⑩ 单击“完成”按钮, 显示如图 22-23 所示“Exchange Server 2007”对话框, 提示需重新启动计算机才能投入使用。



图 22-22 完成



图 22-23 提示重新启动计算机

22.3 配置 Exchange Server 2007

将 Exchange 2007 应用到生产环境之前, 必须进行详细配置, 确保 Exchange 服务器能高效地提交各项服务。在此之前, 应先通过查阅日志, 确认 Exchange 服务器是否安装成功, 如果安装了中心传输服务器角色或边缘传输服务器角色, 则还应验证代理配置。

22.3.1 部署“所有 Exchange 服务器”

依次选择“开始→程序→Microsoft Exchange Server 2007→Exchange 管理控制台”, 打开如图 22-24 所示“Exchange 管理控制台”窗口, 在“完成部署”和“端到端情况”选项卡中, 将指导需要完成的配置任务。

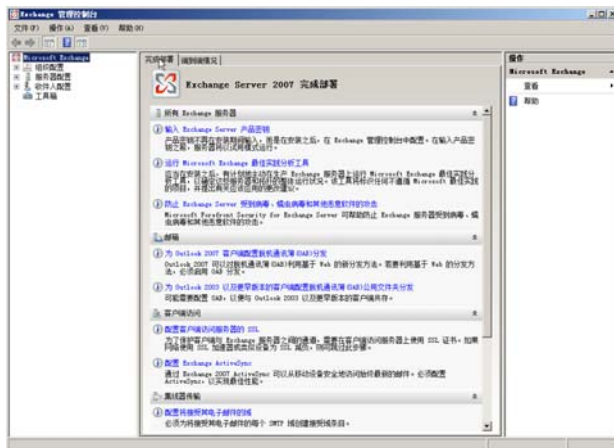


图 22-24 Exchange 管理控制台

- ① 单击“输入 Exchange 产品密钥”链接, 显示如图 22-25 所示的“输入 Exchange 产品密钥”对话框, 按照所叙述的步骤操作即可。
- ② 单击“运行 Microsoft Exchange 最佳实践分析工具”链接, 显示如图 22-26 所示的“运行 Microsoft Exchange 最佳实践分析工具”对话框, 按照步骤操作即可。

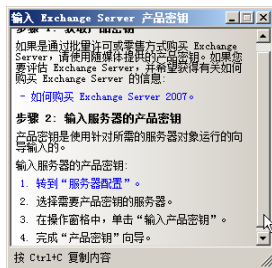


图 22-25 输入 Exchange Server 产品密钥

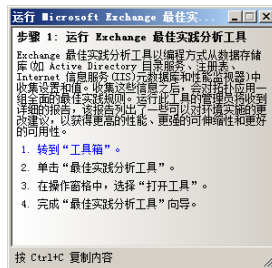


图 22-26 运行 Microsoft Exchange 最佳实践分析工具

③ 转到“工具箱”后，单击“最佳实践分析工具”链接，在打开窗口中选择“打开工具”选项，显示如图 22-27 所示“欢迎使用 Exchange 最佳实践分析工具”窗口，根据需要按照向导操作完成即可。

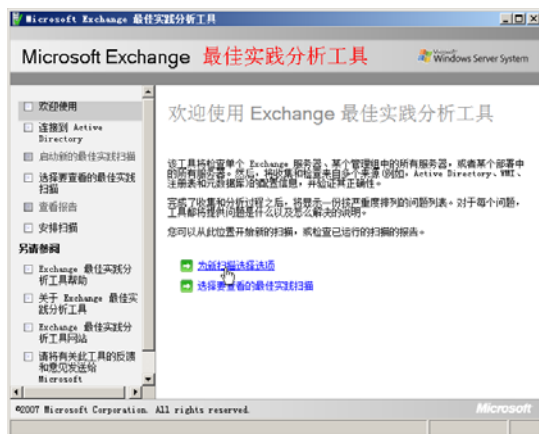


图 22-27 欢迎使用 Exchange 最佳实践分析工具

④ 配置“防止 Exchange Server 受到病毒、蠕虫和其他恶意软件的攻击”选项之前，需要先安装 Microsoft Forefront Security for Exchange Server 工具，这里不作详细介绍。

22.3.2 配置脱机通信簿及公用文件夹分发

在 Exchange Server 2007 中，为了使客户端计算机能够使用 Web 方式登录邮箱，必须启用基于 Web 的分发和公用文件夹分发。具体操作步骤如下。

① 在“Exchange 管理控制台”窗口中，依次展开“组织配置”→“邮箱”，在主窗口中选择“脱机通信簿”选项卡，如图 22-28 所示。

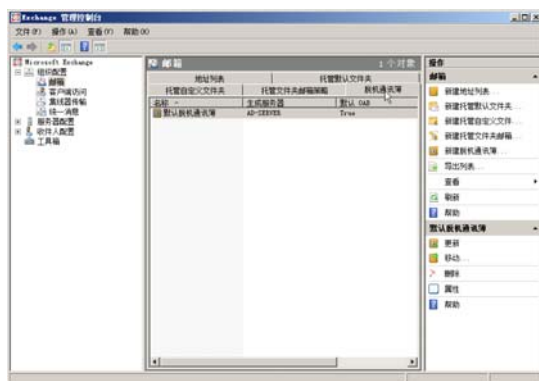


图 22-28 脱机通信簿

② 右击“默认脱机通信簿”选项，选择快捷菜单中的“属性”选项，显示如图 22-29 所示“默认脱机通信簿属性”对话框，切换到“分发”选项卡，选中“启用基于 Web 的分发”和“启用公用文

件夹分发”复选框。

③ 单击“添加”按钮，显示如图 22-30 所示“选择 OAB 虚拟目录”对话框，选择需要添加的虚拟目录即可。

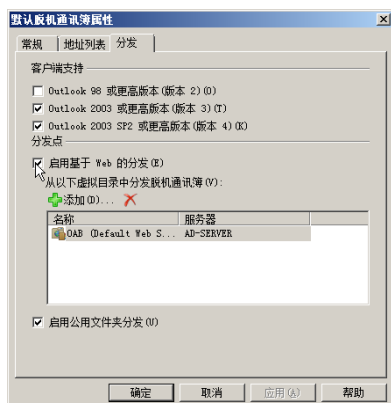


图 22-29 默认脱机通信簿属性

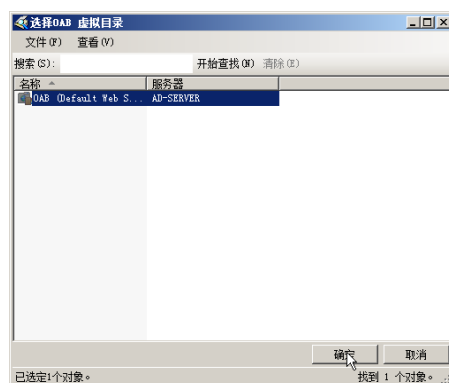


图 22-30 选择 OAB 虚拟目录

④ 单击“确定”按钮，返回“默认脱机通信簿属性”对话框，单击“确定”按钮完成设置。

22.3.3 “客户端访问”的部署

为了使客户端能够安全地访问 Exchange 服务器，可以配置客户端安全策略，包括 SSL 访问、Exchange ActiveSync、新用户和现有用户邮箱策略等。

1. 配置 SSL 访问

为了保护客户端与 Exchange 服务器之间的通道，需要在“客户端访问服务器”上使用 SSL 证书。默认情况下，IIS 会对脱机通信簿虚拟目录之外的所有虚拟目录都要求 SSL，但是，可以为每项客户端访问功能配置其他虚拟目录，此时必须确认每个虚拟目录都配置为要求 SSL。客户端访问的虚拟目录如下：

Outlook Web Access 2007 和 Outlook Web Access 2007 虚拟目录分别为 exchange 和 owa、WebDAV 为 public、ActiveSync 虚拟目录为 Microsoft-Server-ActiveSync、Outlook Anywhere 为 Rpc、自动发现虚拟目录为 Autodiscover、Exchange Web 服务为 EWS、统一消息虚拟目录为 Unified Messaging、脱机通信簿为 OAB。

在 IIS 管理器中，管理员可以配置所有将要使用的客户端访问虚拟目录，步骤如下。

① 依次选择“开始”→“程序”→“管理工具”→“Internet 信息服务 (IIS) 管理器”选项，打开“Internet 信息服务 (IIS) 管理器”控制台。

② 在“默认网站”下选择相应的虚拟目录（以“owa”为例），在主窗口中选择“SSL 设置”选项，如图 22-31 所示。

③ 双击“SSL 设置”，打开如图 22-32 所示的“SSL 设置”窗口，选中“要求 SSL”和“需要 128 位 SSL”复选框。



图 22-31 选择 SSL 设置

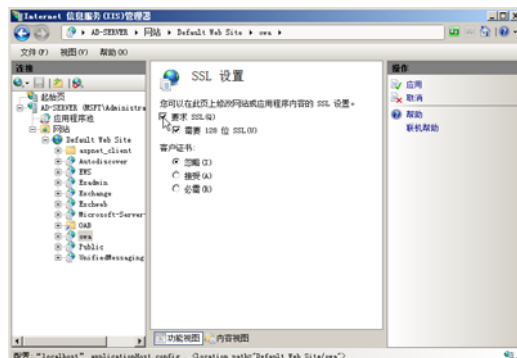


图 22-32 SSL 设置

- ④ 单击“应用”按钮，保存设置即可。
- ⑤ 按照上述步骤对其他虚拟目录进行同样的设置即可。

2. 配置 Exchange ActiveSync

通过 Exchange 2007 ActiveSync 可以从移动设备安全地访问最新的邮件。若用户的环境中配备了运行 Windows Mobile 5.0 和邮件安全及功能包，以及更高版本 Windows Mobile 软件和移动设备，需要配置 Exchange ActiveSync。

① 在 Exchange 管理控制台中，依次展开“组织配置”→“客户端访问”，可以看到一个默认的 Exchange ActiveSync 邮箱策略，如图 22-33 所示。

② 单击“新建 Exchange ActiveSync 策略”链接，显示如图 22-34 所示“新建 Exchange ActiveSync 邮箱策略”对话框，添加邮箱策略名并根据需要进行相应的设置。通常情况下，选中“允许不可设置的设备”和“允许将附件下载到设备”复选框即可。若用户需要设置密码，也可以选中“要求提供密码”复选框，进行相应设置。

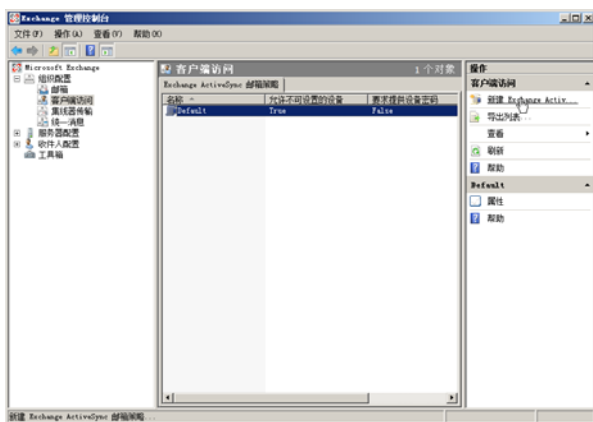


图 22-33 客户端访问



图 22-34 新建 Exchange ActiveSync 策略

3. 配置新用户邮箱策略

为了保护用户邮箱的安全性，应当使新创建的用户邮箱使用 Exchange ActiveSync 邮箱策略。

① 在 Exchange 管理控制台中，选择“收件人配置”选项，显示如图 22-35 所示的“收件人配置”窗口。

② 单击“新建邮箱”链接，启动“新建邮箱”向导，显示如图 22-36 所示的“简介”对话框。可以选择想要创建的邮箱类型，本例选择“用户邮箱”单选按钮。

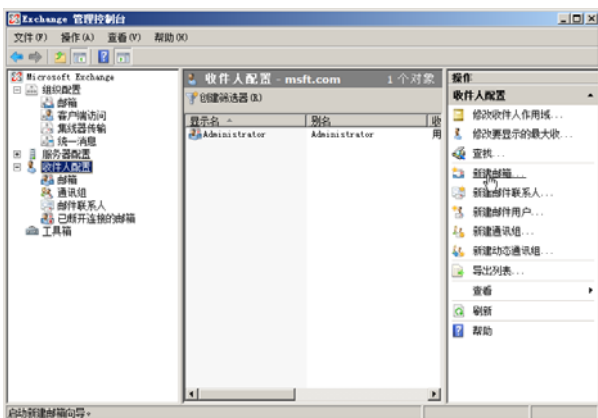


图 22-35 收件人配置



图 22-36 简介

③ 单击“下一步”按钮，显示如图 22-37 所示“用户类型”对话框，选择“新建用户”单选按钮。

④ 单击“下一步”按钮，显示如图 22-38 所示“用户信息”对话框，输入相应的信息即可，如用户名和登录密码等。



图 22-37 用户类型



图 22-38 用户信息

⑤ 单击“下一步”按钮，显示如图 22-39 所示“邮箱设置”对话框，单击“浏览”按钮，选择邮箱数据库，选中“Exchange ActiveSync 邮箱策略”复选框，通过“浏览”按钮选择所需的邮箱策略。

⑥ 单击“下一步”按钮，显示如图 22-40 所示“新建邮箱”对话框。



图 22-39 邮箱设置



图 22-40 新建邮箱

4. 配置现有用户邮箱策略

虽然新用户可以使用邮箱策略，但默认情况下，现有的用户并不会自动使用邮箱策略，需要管理员为现有用户配置邮箱策略。

① 在 Exchange 管理控制台中，依次选择“收件人配置”→“邮箱”选项，选中要添加到 Exchange ActiveSync 邮箱策略的用户（以 test1 用户为例），如图 22-41 所示。

② 单击“属性”链接，显示如图 22-42 所示“test1 属性”对话框，切换到“邮箱功能”选项卡，选择“Exchange ActiveSync”选项。

③ 单击“属性”按钮，显示如图 22-43 所示“Exchange ActiveSync 属性”对话框。

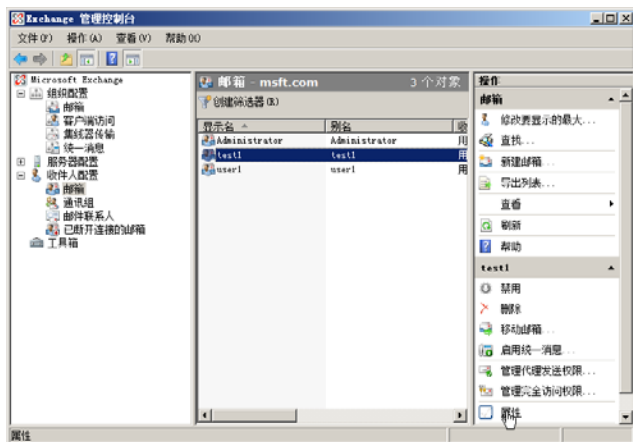


图 22-41 邮箱

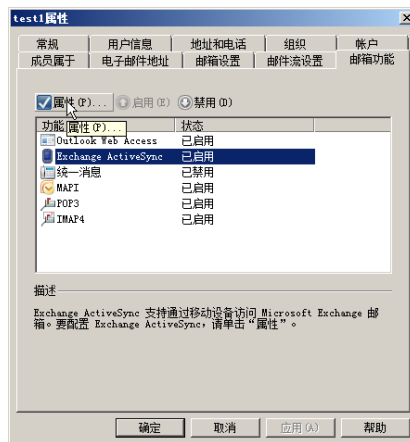


图 22-42 test1 属性

④ 单击“浏览”按钮，显示如图 22-44 所示“选择 ActiveSync 邮箱策略”对话框，选择要应用的策略即可。

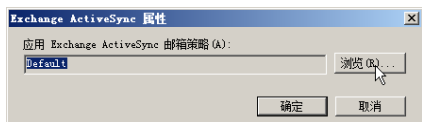


图 22-43 Exchange ActiveSync 属性

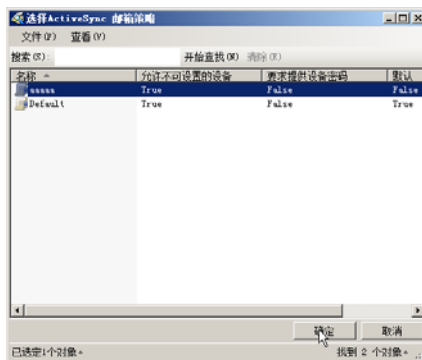


图 22-44 选择 ActiveSync 邮箱策略

⑤ 连续单击“确定”按钮，即可完成配置。

22.3.4 部署“集线器传输”

Microsoft Exchange Server 2007 集线器传输服务器角色，被部署在 Active Directory 目录服务内，它可以提供如下功能。

邮件流：在邮件传递到组织内的收件人收件箱，或者路由到组织外部的用户之前，集线器传输服务器在 Exchange 2007 组织内部发送的所有邮件。

分类：分类程序对通过 Exchange 2007 传输管道移动的所有邮件，执行收件人解析、路由解析和内容转换。

路由：集线器传输服务器确定在组织中发送和接收的所有邮件的路由路径。

传递：邮件由存储驱动程序传递到收件人的邮箱中，组织中的用户所发送的邮件由存储驱动程序从发件人的发件箱中分拣出来，并放在集线器传输服务器上的提交队列中。

1. 创建发送连接器

在 Exchange 2007 传输服务器向目标地址发送邮件的过程中，需要通过发送连接器将邮件传递到下一个跃点。发送连接器控制从发送服务器到接收服务器（或目标电子邮件系统）的出站连接。默认情况下，在安装集线器传输服务器或边缘传输服务器时，不创建任何形式发送连接器。但是，使用基于 Active Directory 目录服务站点拓扑自动计算的不可见隐式发送连接器，在集线器传输服务器之间，以内部方式路由邮件。只有当使用边缘订阅过程将边缘传输服务器订阅到 Active Directory 站点之后，

才能建立端到端邮件流。其他方案必须手动配置连接器，才能建立端到端邮件流。

与 Exchange 2003 有所不同，Exchange 2007 默认安装后只有接收连接器，创建邮箱用户还不能对 Internet 的集线器传输服务器，或者未订阅的边缘传输服务器的客户端发送邮件，用户需要在该服务器上创建一个发送连接器，以便发送邮件。

① 打开“Exchange 管理控制台”窗口，依次选择“组织配置”→“集线器传输”选项，显示如图 22-45 所示“集线器传输”窗口。

② 单击“新建发送连接器”链接，启动“新建 SMTP 发送连接器”向导，默认显示如图 22-46 所示“简介”对话框，在“名称”文本框中，输入发送连接器的名称如：link。



图 22-45 集线器传输



图 22-46 简介

③ 单击“下一步”按钮，显示如图 22-47 所示“地址空间”对话框。

④ 单击“添加”按钮，显示如图 22-48 所示“SMTP 地址空间”对话框，在“地址”文本框中键入“*”。



图 22-47 地址空间

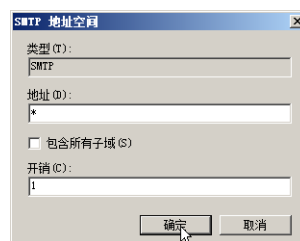


图 22-48 SMTP 地址空间

⑤ 单击“确定”按钮，返回“地址空间”对话框，单击“下一步”按钮，显示如图 22-49 所示“网络设置”对话框。

⑥ 单击“下一步”按钮，显示如图 22-50 所示“源服务器”对话框，单击“添加”按钮，选择希望添加的源服务器即可。

⑦ 单击“下一步”按钮，显示如图 22-51 所示“新建连接器”对话框。

⑧ 单击“新建”按钮，显示如图 22-52 所示“完成”对话框，该发送连接器已经创建成功了，邮箱用户即可收发邮件。



图 22-49 网络设置

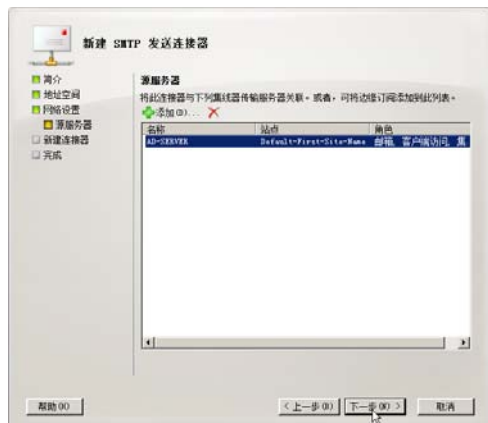


图 22-50 源服务器



图 22-51 新建连接器



图 22-52 完成

2. 创建接受域

作为集线器传输服务器安装的一部分，默认的接受域将作为 Exchange 组织的权威域进行创建。默认的接受域是林根域的完全限定域名 (FQDN)。生产环境中可能需要添加组织的权威域，如与内部 SMTP 域不同的外部 SMTP 域等。

① 打开“Exchange 管理控制台”窗口，依次选择“组织配置”→“集线器传输”选项，切换到“接受域”选项卡，如图 22-53 所示。

② 单击“新建接受域”链接，显示如图 22-54 所示“新建接受域”对话框，键入欲使用的“名称”和“接受域”域名，选择“权威域”单选按钮。



图 22-53 接受域



图 22-54 新建接受域

③ 单击“新建”按钮，接受域创建成功后，会显示“完成”对话框，直接单击“完成”按钮即可。返回“Exchange 管理控制台”可以看到刚刚创建的新的接受域，如图 22-55 所示。

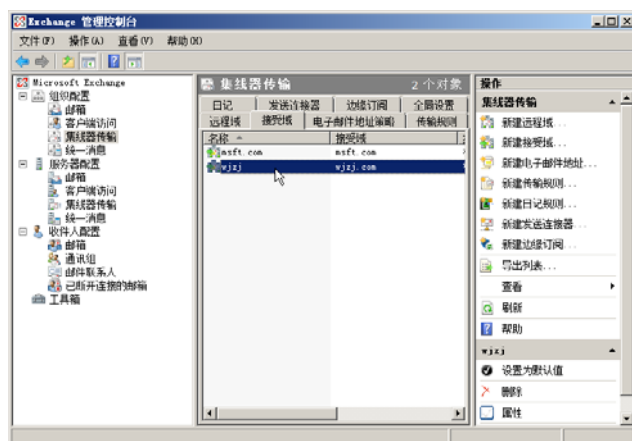


图 22-55 新建的接受域

3. 配置电子邮件策略

在 Exchange Server 2007 中，收件人（包括用户、资源、联系人和组）是 Active Directory 目录服务中任何已启用邮件功能的对象，Exchange 可以向其传递或路由邮件。电子邮件地址策略为收件人生成主电子邮件地址和辅电子邮件地址，以便其可以接收和发送电子邮件。默认情况下，Exchange 包含适用于所有已启用邮件的用户的电子邮件地址策略。此默认策略将收件人的别名指定为电子邮件地址的本地部分，并使用默认的接受域。

① 在“Exchange 管理控制台”窗口中，依次选择“收件人配置”→“邮箱”选项，在主窗口中选择需要更改策略的邮箱用户，例如：test1，如图 22-56 所示。

② 单击“属性”链接，显示如图 22-57 所示“test1 属性”对话框，切换到“电子邮件地址”选项卡。

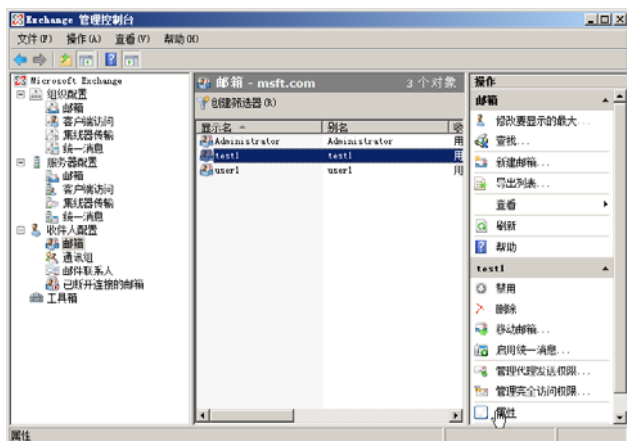


图 22-56 邮箱

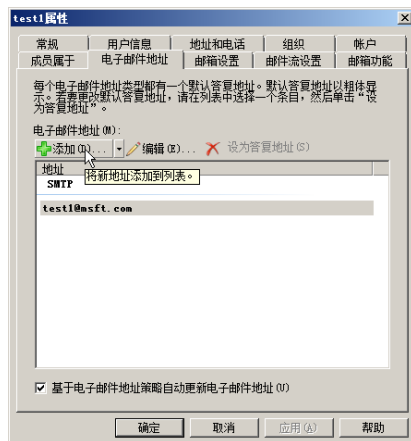


图 22-57 邮箱属性

③ 单击“添加”按钮，显示如图 22-58 所示“SMTP 地址”对话框，在“电子邮件地址”文本框中键入要设置的电子邮件名称，例如：test1.test1@msft.com。

④ 单击“确定”按钮，返回“test1 属性”对话框，新创建的两个电子邮件地址已经显示在列表中，如图 22-59 所示。

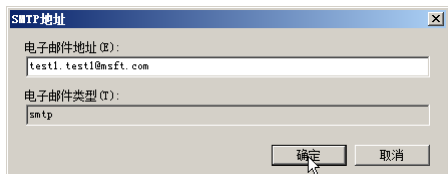


图 22-58 SMTP 地址

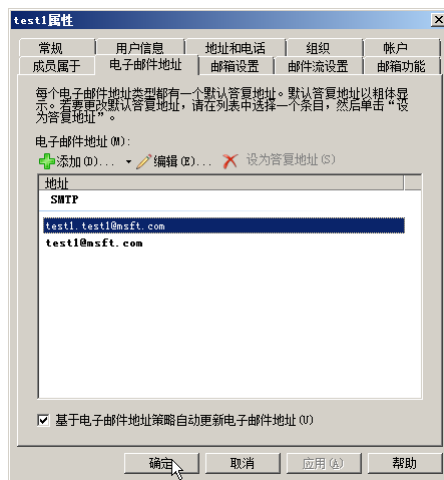


图 22-59 创建成功

- ⑤ 单击“确定”按钮，保存设置。

在上述实例中，编辑的是默认的电子邮件地址策略。用户也可以新建一个电子邮件地址策略，具体步骤如下。

① 在“Exchange 管理控制台”窗口中，依次展开“组织配置”→“集线器传输”选项，在右侧的操作窗格中单击“新建电子邮件策略”链接，启动“新建电子邮件地址策略”向导，默认显示如图 22-60 所示“简介”对话框。在“名称”文本框中，键入创建的策略名称，例如：policy1，并选择相应的收件人类型，通常为“所有收件人类型”。

② 单击“下一步”按钮，显示如图 22-61 所示“条件”对话框，在“步骤 1：选择条件”列表框中，选择策略要应用的条件，例如“收件人属于某个部门”项等。



图 22-60 简介



图 22-61 条件设定

③ 在“编辑条件”列表中，单击“指定的”链接，显示如图 22-62 所示“指定部门”对话框，输入相应的部门名称，如：财务部，单击“添加”按钮，将其添加到列表中。

④ 单击“确定”按钮，返回“条件”对话框。单击“下一步”按钮，显示如图 22-63 所示的“电子邮件地址”对话框。

⑤ 单击“添加”按钮后的小三角，选择“自定义地址”选项，显示如图 22-64 所示的“自定义地址”对话框，在“电子邮件地址”文本框中，输入电子邮件地址的格式如：%g.%s@msft.com（此处的%g 以及%s 分别表示名和姓），在“电子邮件类型”文本框中，输入 SMTP。

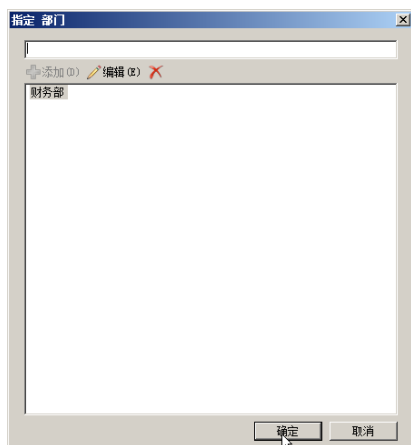


图 22-62 指定 部门



图 22-63 电子邮件地址

⑥ 单击“确定”按钮，返回“电子邮件地址”对话框。单击“下一步”按钮，显示如图 22-65 所示的“日程安排”对话框，可以在这里指定应用该策略的时间及其运行的最长时间，此处选择“立即”单选按钮。

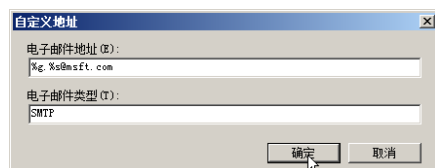


图 22-64 自定义地址



图 22-65 日程安排

⑦ 单击“下一步”按钮，显示如图 22-66 所示“新建电子邮件策略”对话框。
⑧ 单击“新建”按钮，开始创建电子邮件策略。完成后显示“完成”对话框，单击“完成”按钮，新策略即可创建完成，并显示在管理控制台中，如图 22-67 所示。



图 22-66 新建电子邮件策略

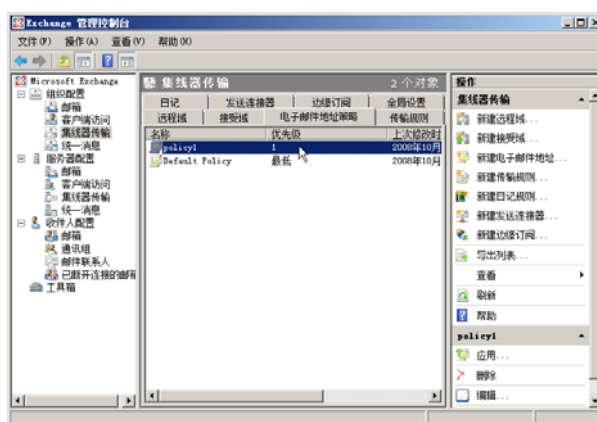


图 22-67 新创建的策略

22.3.5 设置默认用户邮箱大小

在 Exchange 邮件中, 管理员可以设置“默认”用户的邮箱大小, 也可以单独设置每个用户的邮箱大小。

(1) 打开“Exchange 管理控制台”窗口, 依次选择“服务器配置”→“邮箱”选项, 在“数据库管理”选项卡中, 展开“First Storage Group (第一个存储组)”选项, 如图 22-68 所示

(2) 右击“Mailbox Database (邮箱数据库)”, 选择快捷菜单中的“属性”选项, 显示如图 22-69 所示“邮箱数据库属性”对话框, 切换到“限制”选项卡。

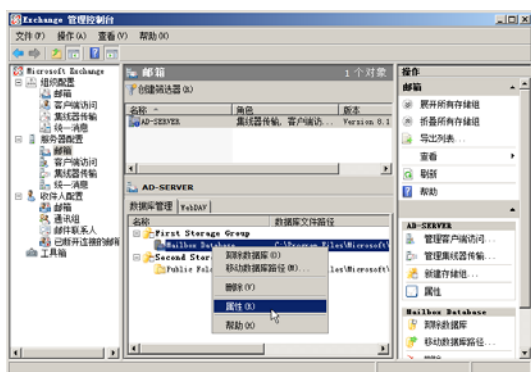


图 22-68 邮箱数据库

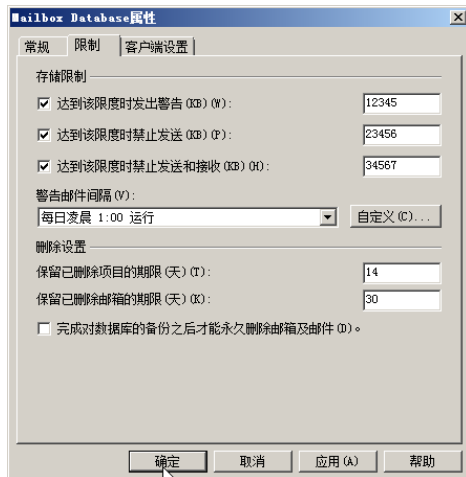


图 22-69 邮箱数据库属性

在此对话框中即可设置“存储限制”和“删除设置”。如果选择“达到该限时发出警告”复选框并在其文本框中设置大小, 则用户的邮箱空间到达此值时, 就会收到系统管理员发来的警告邮件, 但此时用户依然可以收发邮件; 如果选择“达到该限制时禁止发送”复选框并设置大小, 则用户的邮箱空间到达此值后将禁止发送邮件, 但此时可以接收邮件; 如果选择“进行该限时禁止发送和接收”复选框并设置此值, 则到达限制值后用户不能收发邮件, 只能删除无用邮件, 降低空间的使用后才能继续使用邮箱。



提示

通常情况下, 这 3 个值是依次递加的。在“警告邮件间隔”列表中选择(对超过警告空间的用户)发送邮件的时间, 通常选择网络使用率低的时候发送, 例如每天的午夜、凌晨的某个时刻。

在“删除设置”选项组中可以指定何时将已经删除的邮件和邮箱从 Exchange 服务器中永久删除。如果将“保留已删除项目的期限”设置为 0, 表示立即从服务器上永久删除已删除项目, 如果设置为特定值, 则表示保留相应的天数后再从服务器上永久删除。在“保留已删除邮箱的期限”中可以设置从 0~24 855 之间的数值, 设置为 0 时表示立即删除。此项表示在永久删除邮箱之前, 它们在服务器上保留的天数。如果选择了“完成对存储的备份之后才永久删除邮箱及项目”则表示将已删除的邮箱和项目保存在服务器备份之前不能删除, 只有在完成备份之后, 才根据设置删除邮箱和项目。

22.3.6 设置单个邮件大小

在 Exchange 邮件系统中, 还需要设置每个邮箱允许收到(和/或发送)的单个邮件的大小, 通常的邮件系统设置为最大 10 MB。用户可以根据实际需求, 并结合网络带宽, 设置适当的允许值。除此之外, 还可以设置邮件大小、收件人、发件人和连接筛选等信息。

1. 传输设置

① 在“Exchange 管理控制台”窗口中，依次选择“组织配置”→“集线器传输”选项，切换到“全局设置”选项卡，如图 22-70 所示。

② 右击“传输设置”选项，选择快捷菜单中的“属性”选项，显示如图 22-71 所示“传输设置属性”对话框，在“传输限制”选项区域，可以对接收及发送邮件的大小进行设置，包括如下 3 项。

最大接收大小：此项可以设置用户接收邮件的大小限制，其默认为 10 240 KB，即 10M，根据网络带宽和用户要求，可以改变可接收邮件的大小，例如设置为 2 048 KB。

最大发送邮件：此项可以设置用户发送邮件的大小限制，默认为 10 240 KB，同样管理员可以根据带宽及用户要求改变可发送邮件的最大限制，例如 2 048 KB。

最大收件人数：此项可以设置收件人数的大小限制，默认为 5 000 个，根据需要可以改变相应设置。

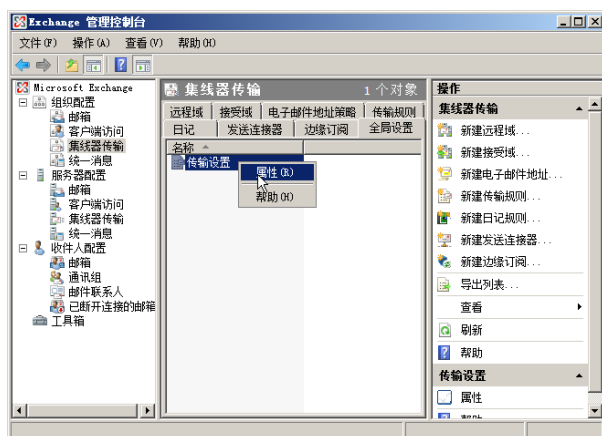


图 22-70 全局设置

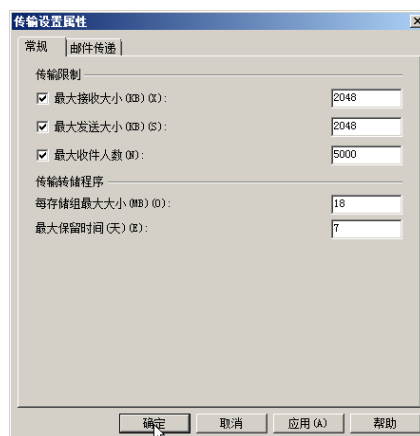


图 22-71 传输设置属性

2. 发送单一邮件的大小限制

① 在“Exchange 管理控制台”窗口中，依次选择“组织配置”→“集线器传输”选项，切换到“发送连接器”选项卡，如图 22-72 所示。

② 右击创建的“link”连接器，选择快捷菜单中的“属性”选项，显示如图 22-73 所示“link 属性”对话框，在“常规”选项卡中，选中“最大邮件大小为 (KB)”复选框，并输入希望限制的具体数值，如 10 240 (表示 10 M)。



图 22-72 发送连接器

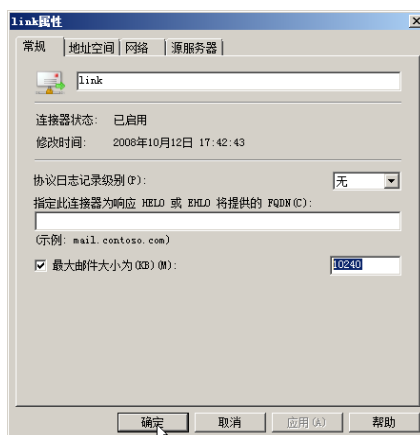


图 22-73 link 属性

③ 单击“确定”按钮，保存设置。

3. 接收单一邮件的大小限制

安装好中心传输服务器后，系统会自动建立两个接收连接器，分别为 Client Server 和 Default Server。Client Server 连接器主要用来接收使用 POP 3 或 IMAP 4 的客户端应用程序所提交的电子邮件。默认情况下，该接收连接器配置为通过 TCP 端口 587 接收电子邮件。Default Server 连接器主要用来接受来自边缘传输服务器的连接，用以接收来自 Internet 和其他中心传输服务器的邮件。默认情况下，该接收连接器配置为通过 TCP 端口 25 接收电子邮件。

① 在“Exchange 管理控制台”窗口中，依次选择“服务器配置”→“集线器传输”选项，如图 22-74 所示。

② 在主窗口中右击“Default AD-Server”，选择快捷菜单中的“属性”选项，显示如图 22-75 所示“Default AD-Server 属性”对话框，在最下方的“最大邮件大小为 (KB):”编辑栏中输入将要设置的数值如：20 480（表示最大接收邮件大小为 20 MB）。



图 22-74 Default AD-Server

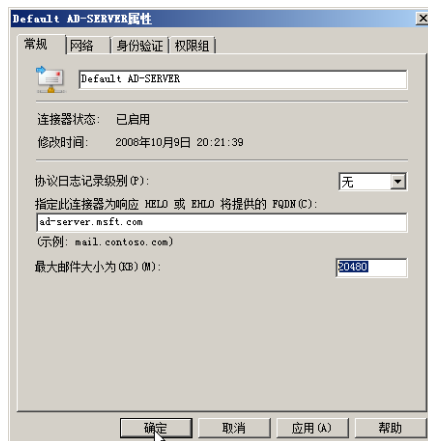


图 22-75 Default AD-Server 属性

③ 单击“确定”按钮，保存设置。

Client Server 的设置方法与上述步骤相同，此处不再赘述。

22.3.7 HELO 信息设置

在邮件服务器中，必须正确设置外发的 HELO（或 EHLO）信息，如果不能正确设置这些信息，会被许多邮件服务器拒绝，邮箱系统外发的信件就会被一些启用“DNS 反向域名解析”的邮件服务器拒收。



如果网络中有多台 Exchange Server，需要在每台 Exchange 服务器上设置 HELO 信息，本处以 ad-server 为例介绍其设置方法。

① 在“Exchange 管理控制台”窗口中，依次选择“组织配置”→“集线器传输”选项，切换到“发送连接器”选项卡，如图 22-76 所示。

② 右击要设置的发送连接器，如 link，选择快捷菜单中的“属性”选项，显示如图 22-77 所示“link 属性”对话框，在“指定此连接器为响应 HELO 或 EHLO 将提供的 FQDN”文本框中，输入集线器服务器的名称，由于所有邮箱服务器角色都安装在了 AD-Server 这台计算机上，所以此处应为 ad-server.msft.com。

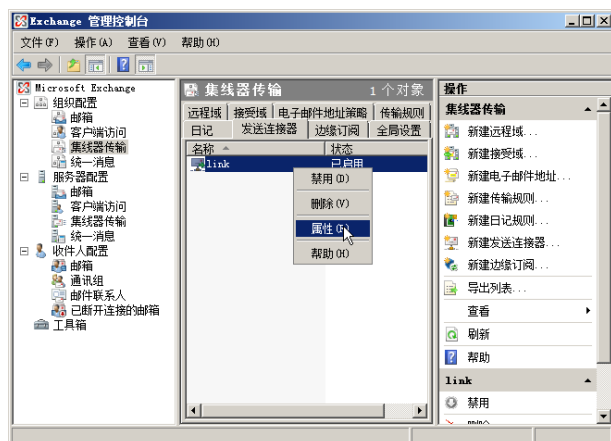


图 22-76 发送连接器

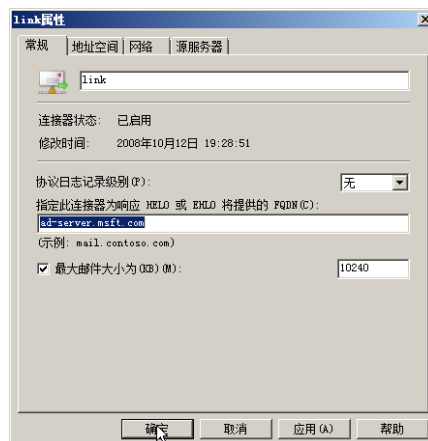


图 22-77 link 属性

- ③ 单击“确定”按钮，保存设置。

22.3.8 公用文件夹设置

公用文件夹是专门为共享访问设计的，为收集、组织信息及与您的工作组或组织中的其他人共享信息，提供了一种轻松、有效的方式。公用文件夹是分层组织的，存储在专用数据库中，并且可以在 Exchange 服务器之间进行复制。在 Exchange Server 2007 中，公用文件夹是一个可选功能。如果网络中的所有客户端计算机全部使用 Office Outlook 2007，则对于诸如忙/闲信息和脱机通信簿（OAB）下载等功能，不存在对公用文件夹的任何依赖。在 Exchange 2007 中，不使用公用文件夹实现 OAB 下载和忙/闲信息，而是通过自动发现服务、Microsoft Exchange 系统助理服务和 Microsoft Exchange 文件分发服务实现这些功能。若要连接到 Exchange 来实现 OAB 和 Schedule+忙/闲功能，则运行 Outlook 2003、Outlook 2002、Outlook 2000 或 Outlook 98 的所有客户端计算机，都需要部署公用文件夹。

1. 新建公用文件夹

运行 Outlook 2003 及更早版本或 Microsoft Entourage 的计算机，需要使用公用文件夹数据库才能连接到 Exchange 2007。因此，在纯 Exchange 2007 网络中，当在第一个服务器上安装邮箱服务器角色时，安装程序会提示如图 22-78 所示的问题：“您的组织中是否存在任何正在运行 Outlook 2003 以及更早版本或 Entourage 的客户端计算机？”如果回答“是”，则会创建公用文件夹数据库。如果回答“否”，则不会创建公用文件夹数据库。



图 22-78 客户端设置

- ① 打开 Exchange 管理控制台，选择“工具箱”选项，显示如图 22-79 所示的“工具箱”窗口。
- ② 在主窗口中右击“公用文件夹管理控制台”，选择快捷菜单中的“打开工具”选项，显示如图 22-80 所示“公用文件夹管理控制台”对话框。



图 22-79 工具箱

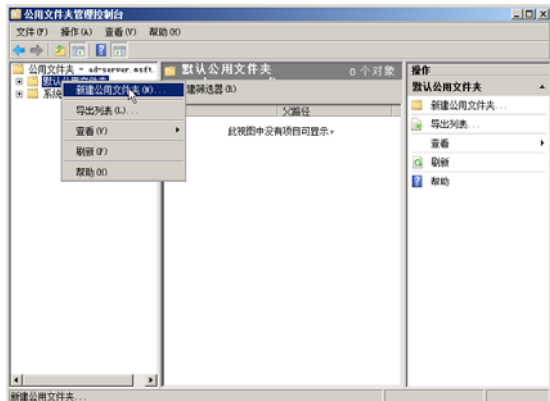


图 22-80 公用文件夹管理控制台

- ③ 右击“默认公用文件夹”，选择快捷菜单中的“新建公用文件夹”选项，显示如图 22-81 所示的“新建公用文件夹”对话框，键入要创建的文件夹的名称，如：财务部。



图 22-81 新建公用文件夹

- ④ 单击“新建”按钮，创建完成。

2. 配置公用文件夹复制

公用文件夹复制是一个过程，公用文件夹内容和层次结构可通过该过程跨多个服务器进行复制，从而提高效率和容错能力。如果分别位于各个独立服务器上的多个公用文件夹数据库，都支持一个单一公用文件夹树，则 Exchange 将使用公用文件夹复制保持数据库同步。如果组织中存在多个公用文件夹数据库，则无法使用群集连续复制（CCR）、本地连续复制（LCR）或备用连续复制（SCR）。如果组织中存在两个或更多公用文件夹数据库，即使尚未配置要复制的公用文件夹，也将进行公用文件夹复制。公用文件夹复制和存储组复制不能组合使用。因此，CCR、LCR 和 SCR 仅在组织中没有其他公用文件夹数据库的情况下对公用文件夹数据库可用。

- ① 在“公用文件夹管理控制台”窗口中，右击欲设置的公用文件夹，如“财务部”，选择快捷菜单中的“属性”选项，显示如图 22-82 所示的“财务部属性”对话框，切换到“复制”选项卡。
- ② 单击“添加”按钮，显示如图 22-83 所示的“选择公用文件夹数据库”对话框，选择要在其上复制公用文件夹的公用文件夹数据库即可。
- ③ 单击“确定”按钮，返回“财务部属性”对话框，继续单击“确定”按钮保存设置即可。

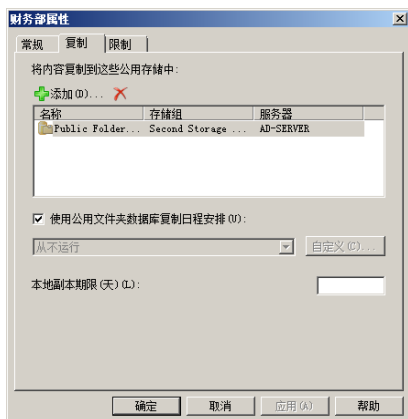


图 22-82 财务部属性

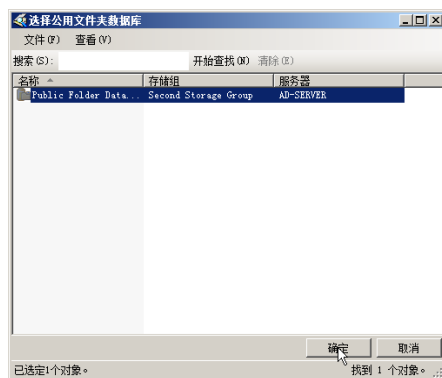


图 22-83 选择公用文件夹数据库

默认情况下，Exchange 使用为公用文件夹数据库设置的复制日程安排。若要为公用文件夹创建自定义复制日程安排，在“财务部属性”对话框中清除“使用公用文件夹数据库复制日程安排”复选框，并使用自己定义的日程安排。

3. 复制邮件的大小限制

- ① 在“Exchange 管理控制台”窗口中，依次选择“服务器配置”→“邮箱”选项，在“数据库管理”选项卡中，选择欲设置的公用文件夹数据库，如图 22-84 所示。
- ② 右击公用文件夹数据库并选择“属性”选项，显示如图 22-85 所示的“Public Folder Database 属性”对话框，切换到“复制”选项卡，在“复制邮件大小限制值(KB)”文本框中，键入邮件大小限制，该值的范围为 1~2 097 151KB。

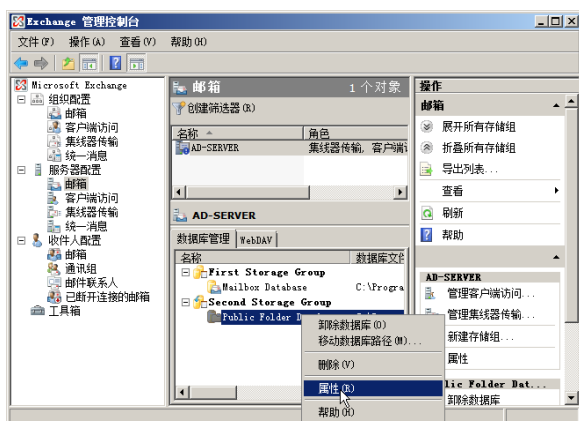


图 22-84 数据库管理

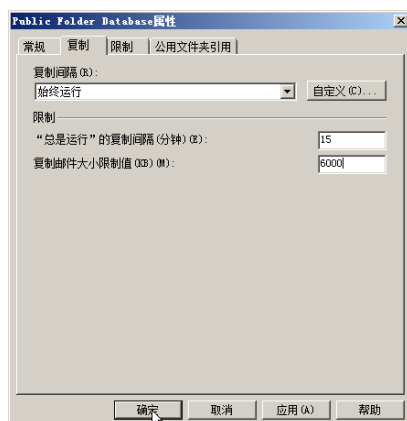


图 22-85 Public Folder Database 属性

- ③ 单击“确定”按钮，保存设置。

22.4 用户管理

为了使用户能够使用 Exchange Server 2007 收发邮件，必须先在 Exchange Server 2007 中添加用户并创建用户邮箱，并为用户设置邮件地址、限制邮箱大小并配置邮箱功能。同时，由于用户数量可能比较多，为了便于管理，还应创建不同的通信组。

22.4.1 同时创建用户和邮箱

管理员在创建用户以后，可以为用户指定邮箱，也可以在创建用户的同时，就为用户创建邮箱，并为用户指定邮箱策略。

① 在“Exchange 管理控制台”窗口中，依次选择“收件人配置”→“邮箱”选项，单击“新建邮箱”链接，启动“新建邮箱”向导，如图 22-86 所示。选择“用户邮箱”单选按钮。

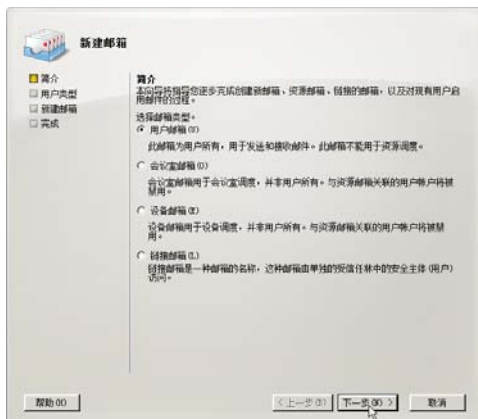


图 22-86 简介

② 单击“下一步”按钮，显示如图 22-87 所示“用户类型”对话框，选择“新建用户”单选按钮。

③ 单击“下一步”按钮，显示如图 22-88 所示“用户信息”对话框，输入必要的用户信息，本例中为 user1 用户。



图 22-87 用户类型



图 22-88 用户信息

④ 单击“下一步”按钮，显示如图 22-89 所示“邮箱设置”对话框。

⑤ 单击“浏览”按钮，显示如图 22-90 所示“选择邮箱数据库”对话框，选择希望使用的数据库。单击“确定”按钮，返回“邮箱设置”对话框，如果需要为新用户应用托管文件夹或 Exchange ActiveSync 邮箱策略，则可以选择相应的复选框。



图 22-89 邮箱设置



图 22-90 选择邮箱数据库

- ⑥ 单击“下一步”按钮，如图 22-91 所示“新建邮箱”对话框。
- ⑦ 单击“新建”按钮，显示如图 22-92 所示“完成”对话框。直接单击“完成”按钮，即可完成新用户的创建。



图 22-91 新建邮箱



图 22-92 完成

22.4.2 为已有用户创建邮箱

如果在安装 Exchange 之前已经创建了用户，那么，就可以利用 Exchange 邮箱服务器的“新建邮箱”向导，为已有用户创建邮箱。

- ① 在“Exchange 管理控制台”窗口中，依次选择“收件人配置”→“邮箱”选项，单击“新建邮箱”链接，在显示的“简介”对话框中，选择“用户邮箱”单选按钮。单击“下一步”按钮，在“用户类型”对话框中，选择“现有用户”单选按钮，如图 22-93 所示。
- ② 单击“添加”按钮，显示如图 22-94 所示“选择用户”对话框，选择要为其创建邮箱的用户，如用户 test1。



图 22-93 用户类型



图 22-94 选择用户

- ③ 单击“确定”按钮，返回“用户类型”对话框，接下来的操作步骤和新建用户邮箱时相同，此处不复赘述。

22.4.3 通信组设置

通信组是已启用了邮件的 Active Directory 目录服务组对象，其主要功能用于加快对电子邮件以及 Exchange 组织中其他信息的大量发送速度。管理员可以使用“收件人配置”下的“通信组”选项，针对多

种通信组执行管理任务，同时也可以创建新的通信组（包括安全组），并修改、删除或禁用现有通信组。

1. 新建通信组

- ① 在“Exchange 管理控制台”窗口中，依次选择“收件人配置”→“通信组”选项，如图 22-95 所示。
- ② 右击“通信组”并选择快捷菜单中的“新建通信组”选项，启动“新建通信组”向导，默认显示如图 22-96 所示“简介”对话框，选择“新组”单选按钮。

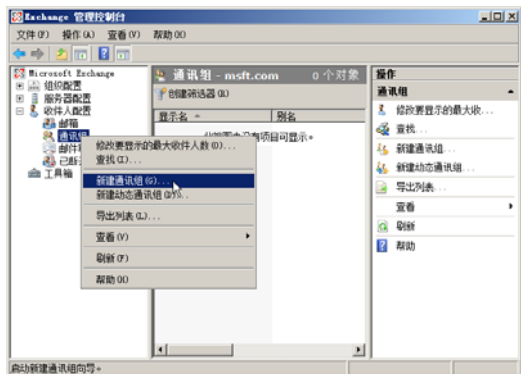


图 22-95 新建通信组



图 22-96 简介

- ③ 单击“下一步”按钮，显示如图 22-97 所示“组信息”对话框，选择“分发”单选按钮，并输入相应的名称，例如 caiwubu。

- ④ 单击“下一步”按钮，显示如图 22-98 所示“新建通信组”对话框。



图 22-97 组信息



图 22-98 新建通信组

- ⑤ 单击“新建”按钮，开始创建。完成后，单击“完成”按钮即可。

2. 通信组属性

当通信组创建完成以后，就可以为通信组添加成员、设置收发邮件的电子邮件地址、设置邮件大小限制及邮件传递限制等。

- ① 在“Exchange 管理控制台”的“通信组”窗口中，右击组名（如 caiwubu）并选择快捷菜单中的“属性”选项，显示如图 22-99 所示“caiwubu 属性”对话框，切换到“成员”选项卡。单击“添加”按钮，在“选择收件人”对话框中选择要添加的组成员即可。
- ② 切换到如图 22-100 所示“电子邮件地址”选项卡，可以为该通信组设置收发邮件的电子邮件地址。
- ③ 切换到如图 22-101 所示“邮件流设置”选项卡，单击“属性”按钮，可以为该通信组设置邮件大小限制及邮件传递限制。

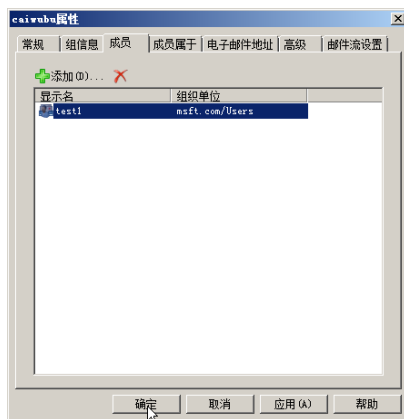


图 22-99 caiwubu 属性

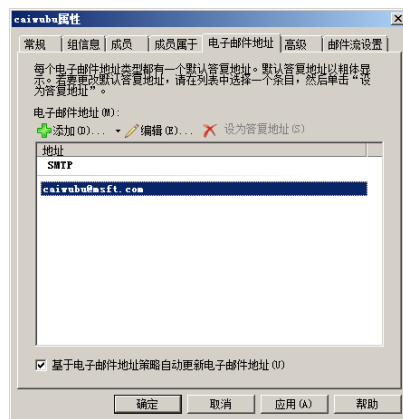


图 22-100 电子邮件地址

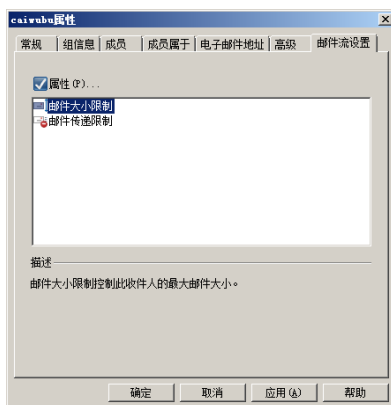


图 22-101 邮件流设置

22.4.4 用户属性

在“Exchange 管理控制台”窗口中，依次选择“收件人配置”→“邮箱”选项，显示了所有已经配置了邮箱的用户，在此处可以设置每个用户属性。这里以 test1 邮箱用户为例，介绍用户属性的设置。

1. 电子邮件地址

在“邮箱”窗口中，右击 test1 用户，选择快捷菜单中的“属性”选项，即可打开用户属性设置对话框。

在“电子邮件地址”选项卡中，可以添加、删除、更改用户的电子邮件地址或其他地址，如图 22-102 所示。单击“添加”按钮，添加另一个地址，或者选中一个地址后，单击“编辑”按钮进行修改。当有多个地址时，可以选择一个地址为主地址，作为用户的默认电子邮件地址。



图 22-102 电子邮件地址

2. 邮箱设置

在用户属性对话框中，选择“邮箱设置”选项卡，如图 22-103 所示，可以为当前用户邮箱配额或邮箱记录管理。如果想单独为当前用户设置邮箱大小限制，则可以选中“存储配额”选项。

单击“属性”按钮，显示如图 22-104 所示“存储配额”对话框，可以为当前用户设置使用邮箱数据库默认设置或自定义其邮箱配额限制。

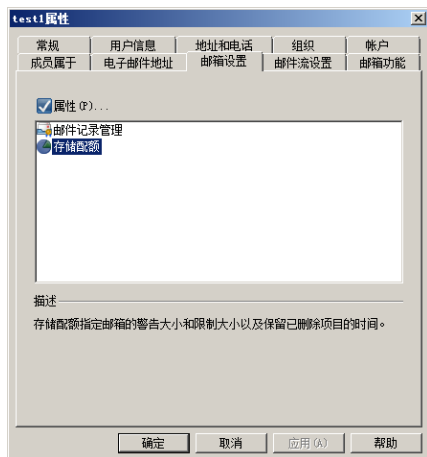


图 22-103 邮箱设置

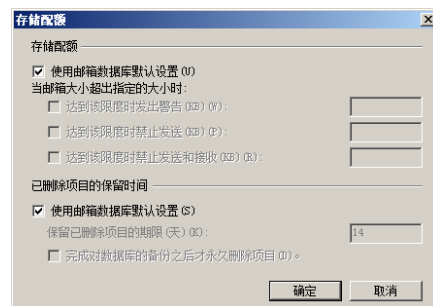


图 22-104 存储配额

3. 邮件流设置

切换到“邮件流设置”此选项卡，如图 22-105 所示，可以为用户设置转发地址、邮件大小限制或邮件传递限制。

如果想为该用户设置转发用户，则可以选中“传递选项”并单击“属性”按钮进行设置；如果想为用户设置邮件大小限制，则可以选择“邮件大小限制”并单击“属性”按钮进行设置；“邮件传递限制”选项可以设置接收或拒收某些发件人的邮件。

4. 邮箱功能

切换到“邮箱功能”选项卡，如图 22-106 所示，可以为邮箱用户启用或禁用各种邮箱功能。在列表中选择功能，单击“属性”按钮，可以更改 Exchange ActiveSync、统一消息、POP3 和 IMAP4 的配置。

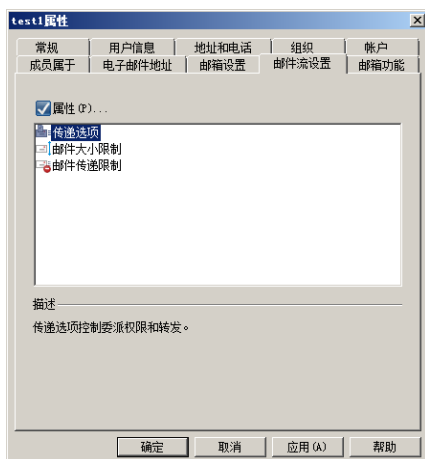


图 22-105 邮箱流设置

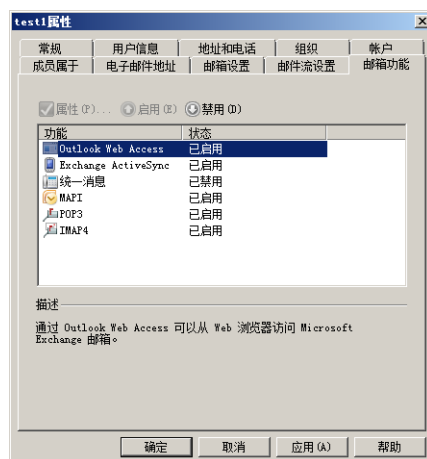


图 22-106 邮箱功能

22.5 客户端的使用

Exchange 的客户端是 Microsoft Outlook 或 Outlook Web Access（简称 OWA），而使用其他电子邮

件客户端程序，如 Outlook Express、Foxmail 等，只能使用 Exchange 的收发邮件功能。对于 Exchange 而言，域客户端上部署的 Office Outlook 2003 可以完全发挥其功能。OWA 能发挥 Exchange 提供的绝大部分功能。

22.5.1 Outlook 2003/Office 2007 的使用

Exchange 和 Outlook 主要应用于企业网络，通常情况下，都是将 Exchange、Outlook 与 Active Directory 配合使用，所以，网络中的工作站都应该加入到域。

1. Outlook 2007 的配置

Office Outlook 2007 可以提供全面的时间和信息管理功能。利用“即时搜索”和“待办事项栏”等新功能，可以组织和随时查找所需信息。通过新增的日历共享功能、Microsoft Exchange 2007 技术以及经过改进的 Microsoft Windows SharePoint Services 3.0 信息访问功能，用户可以与同事、朋友和家人，安全地共享存储在 Office Outlook 2007 中的数据。Office Outlook 2007 可以帮助用户更加轻松地排定优先次序和控制时间，以便将主要精力放在最重要的事情上。

- ① 将需要配置的客户端加入到 Active Directory，并安装 Outlook 2007。
- ② 第一次使用 Outlook 时，将显示 Outlook 2007 的启动向导，如图 22-107 所示。
- ③ 单击“下一步”按钮，显示如图 22-108 所示的“电子邮件账户”对话框，选择“是”单选按钮。



图 22-107 Outlook 2007 启动

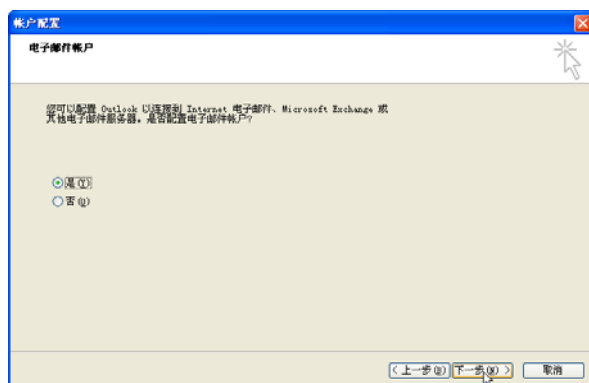


图 22-108 电子邮件账户

- ④ 单击“下一步”按钮，显示如图 22-109 所示的“选择电子邮件服务”对话框，选择“Microsoft Exchange、POP3、IMAP、或 HTTP”单选按钮。

- ⑤ 单击“下一步”按钮，显示如图 22-110 所示的“自动账户设置”对话框，Outlook 2007 会根据系统实际情况，自动填写“您的姓名”和“电子邮件地址”文本框。

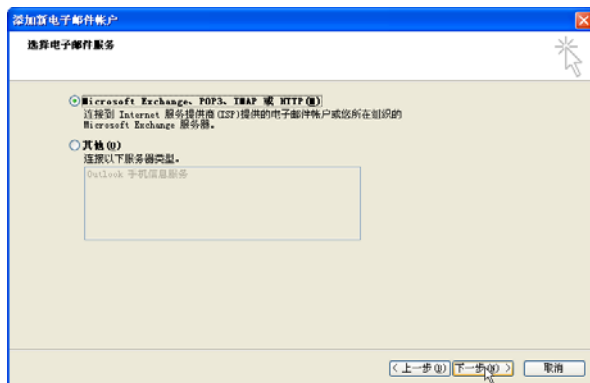


图 22-109 选择电子邮件服务

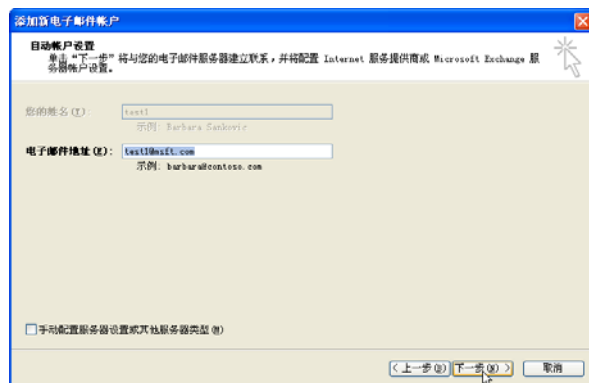


图 22-110 自动账户设置

⑥ 单击“下一步”按钮，显示如图 22-111 所示的“正在配置”对话框，开始建立应用程序到服务器的连接。

⑦ 单击“完成”按钮，即可完成配置向导，同时启动 Outlook 2007，如图 22-112 所示。

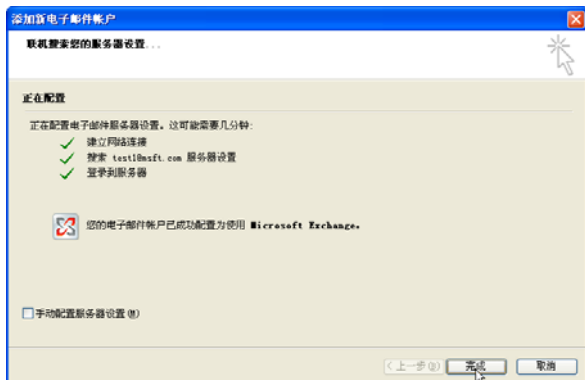


图 22-111 正在配置

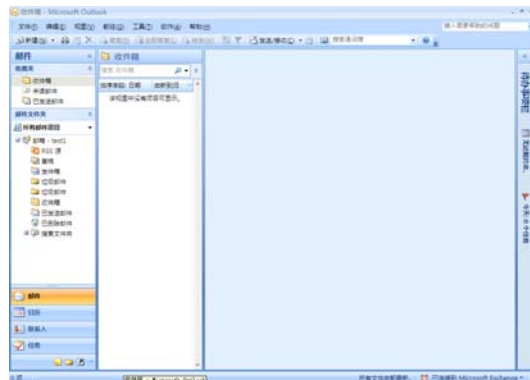


图 22-112 Outlook 2007 主窗口

如果在此之前已经配置过 Outlook 2007，但是并未将其配置为 Exchange Server 的客户端，则可以在“控制面板”中单击“切换到经典视图”选项，双击“邮件”选项，显示如图 22-113 所示的“邮件设置”对话框。

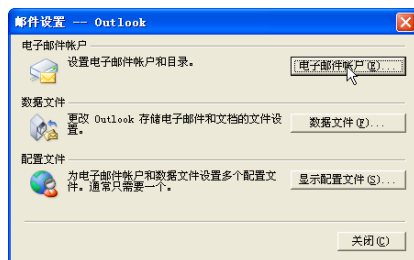


图 22-113 邮件设置

单击“电子邮件帐户”按钮，显示如图 22-114 所示的“账户设置”对话框，切换到“电子邮件”选项卡，在这里即可“删除”、“更改”或“修复”当前邮箱。选择“新建”按钮，显示如图 22-115 所示的“添加新电子邮件帐户”对话框，按默认配置即可，接下来的操作步骤与初始配置 Outlook 2007 时创建邮箱完全相同，此处不复赘述。

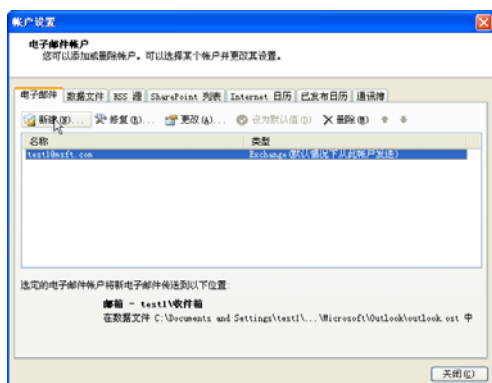


图 22-114 账户设置



图 22-115 添加新电子邮件账户

2. Outlook 2003 的配置

① 第一次运行 Outlook 时，将显示 Outlook 2003 启动向导。单击“下一步”按钮，显示如图 22-116 所示的“电子邮件帐户”对话框，选择“是”单选按钮。

② 单击“下一步”按钮，显示如图 22-117 所示的“服务器类型”对话框，选择“Microsoft Exchange Server”单选按钮。

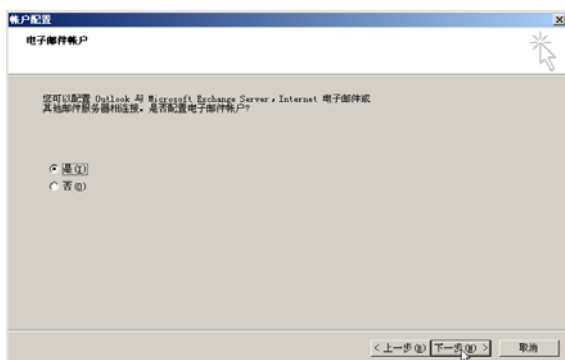


图 22-116 电子邮件账户



图 22-117 服务器类型

③ 单击“下一步”按钮，显示如图 22-118 所示的“Exchange Server 设置”对话框，在“Microsoft Exchange Server”文本框中，输入 Exchange 服务器的计算机名或 IP 地址，在“用户名”文本框中，输入当前登录用户名所属的邮箱名，单击“检查姓名”按钮，如果信息填写正确并且网络畅通，则 Exchange 服务器信息及邮箱将“替换”原来填写的信息。

④ 单击“下一步”按钮，显示如图 22-119 所示的“祝贺您”对话框。



图 22-118 Exchange Server 设置



图 22-119 设置完成

⑤ 单击“完成”按钮，关闭向导，即可完成新客户端配置，同时启动 Outlook 2003，如图 22-120 所示。

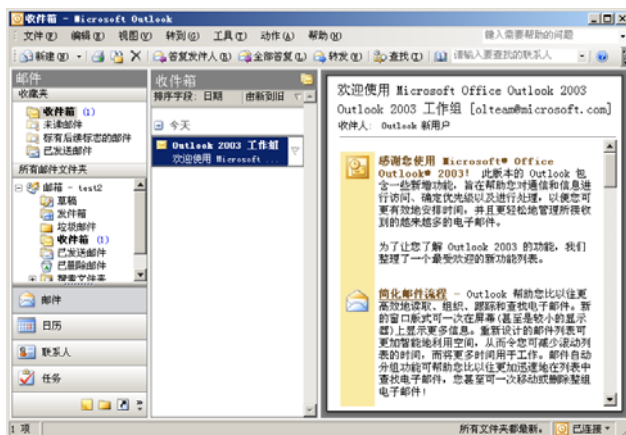


图 22-120 Outlook 2003

现在，即可开始使用 Outlook 2003 收发邮件，用户可以根据自己的需要做进一步的配置。

22.5.2 OWA 的使用

Exchange 还提供了 OWA 访问方式，用户可以在只使用 IE 或其他与 IE 兼容的浏览器的情况下，实现与使用 Outlook 相类似的功能。如果计算机不能连接到网络中的域控制器，或者计算机没有加入到域，或者出差在外的时候，使用 OWA 是另一种替代方案。

① 打开 IE 浏览器，在地址栏中输入 <https://ad-server.msft.com/owa>，回车显示如图 22-121 所示窗口。其中，ad-server 是 Exchange 服务器的计算机名，也可以使用 IP 地址或其 DNS 解析名称代替。

② 输入用户名及密码，单击“登录”按钮，显示如图 22-122 所示的窗口，由于是第一次使用 OWA 方式登录，所以会出现设置时区、界面语言等选项。

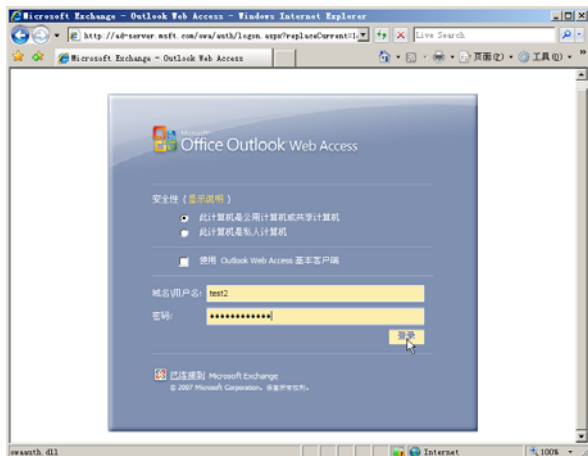


图 22-121 IE 登录方式

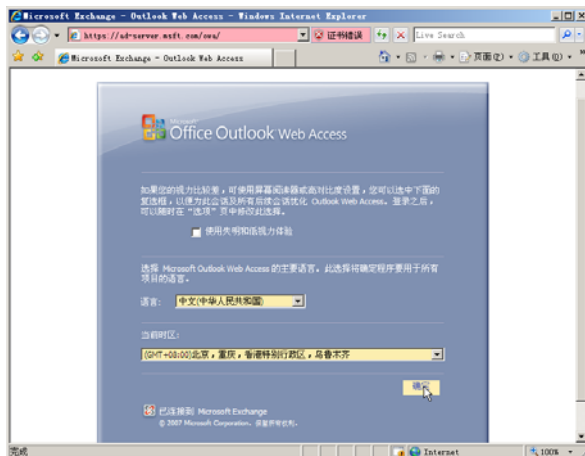


图 22-122 时区选择

③ 单击“确定”按钮，即可以 OWA 方式登录邮箱，如图 22-123 所示。这里操作方法和使用 Outlook 2007 的方法相同。

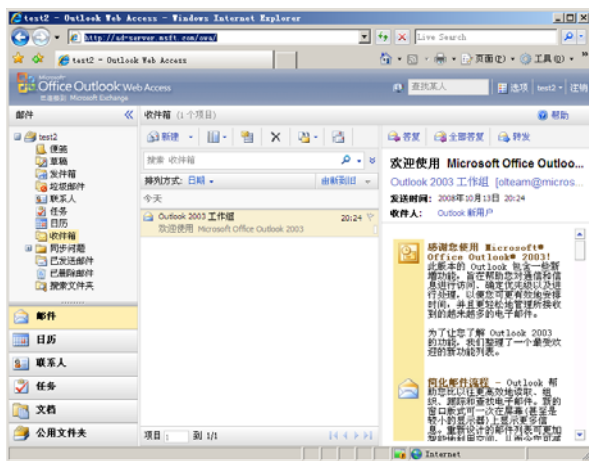


图 22-123 登录成功

第 23 章 OCS 2007 即时消息服务

OCS 2007（全称为 Office Communications Server 2007）是微软首款融合多种应用于一体的企业产品，包括即时通信、会议、VoIP（IP 语音）电话等。相对于其前身 OCS 2005 而言，OCS 2007 提供了更加丰富的功能，加强支持组即时通信和改善部署和管理，OCS 2007 的包括实时会议上托管服务器的防火墙和提供功能齐全的 VoIP 解决方案，可以整合现有的 PBX 基础设施。

23.1 OCS 2007 简介

OCS 2007 是 Microsoft 公司为协助企业增强内部沟通能力，而推出的新一代企业级即时通信平台，例如，人、信息、业务流程相互沟通等，重点强调借助音频、视频、数据即时信息为企业“协同办公”而服务。

►► 23.1.1 OCS 2007 组件

OCS 2007 系统包括服务器端（标准版或企业版）、访问代理服务器、代理服务器、存档服务器、SIP-PSTN 网关、客户端软件等 6 部分，每个部分的功能如下。

1. OCS 2007 服务器端

OCS 2007 包括标准版和企业版两种版本。标准版适用于中小型组织，在不需要 Enterprise Edition 提供的性能、可伸缩性和高可用性的组织中，建议使用标准版。

企业版适用于大型组织常用的大型部署。多个企业版 OCS 服务器可以实现群集，实现网络负载平衡，池中的服务器共享存储用户数据的中央 SQL Server 数据库。

2. 访问代理服务器

访问代理服务器部署在外围网络中，可使局域网能够安全地与其他网络进行连接，并且可以为远程访问的用户提供 OCS 服务。网络中位于企业 Intranet 外部的用户，可以通过 TLS 安全地连接到访问代理服务器来访问 OCS 服务，而不必依赖 VPN 服务。此外，远程机构或分支机构，也可以通过一个采用 MTLS 的本地转发代理服务器连接到访问代理服务器。

3. 代理服务器

用户可以通过两种方式部署代理服务器。

第一种方式是：在具有 OCS 标准版或企业版的域环境中，代理服务器通常被部署为应用程序服务器。在这种环境中，应用程序代理服务器可用于路由过某些应用程序来进行处理。

第二种方式是：在没有部署 OCS 服务器或池的分支机构中，代理服务器可以被部署为转发代理服务器。在该方案中，转发代理服务器将连接到位于中央站点或数据中心站点的访问代理服务器，访问代理服务器然后将通信量发送到其后面的内部 OCS。

4. 存档服务

存档服务主要用于存储组织内部的通信，存储与连接用户之间的通信，以及跟踪整个组织内的使用情况数据。管理员既可以为林中的所有用户全局配置存档设置，也可以为各个用户单独配置存档设置。默认情况下，用户的个别设置将覆盖全局设置。



5. SIP-PSTN 网关

OCS 2007 通过 SIP-PSTN（公用电话交换网）网关支持个人计算机到电话连接。标准版或企业版 OCS 服务器均可以被配置为直接连接到该网关，有两种配置方法。第一种方法是：指定一台独立的服务器作为网关主机，所有呼叫都通过该服务器路由。第二种方法是：部署 OCS 2007 支持的唯一拓扑。

6. 客户端

OCS 2007 的客户端非常丰富，可以是运行在计算机上的 Office Communicator 2007、Microsoft Live Meeting 2007，也可以作为 Web 客户端。

23.1.2 OCS 服务模板

OCS 2007 服务器和客户端，是 OCS 系统中必不可少的组件，而其他组件，管理员可以根据客户需求，结合网络实际情况，选择安装。

1. 标准版池的网络结构

在中小企业网络中，只需要安装 OCS 2007 标准版和客户端软件即可，需要一台 Active Directory 服务器和一台 Office Communication Server 2007 服务器。可以按照如下步骤进行部署。

- ① 将 Windows Server 2003 服务器升级到域，将 OCS 服务器加入域，同时提升为额外域控制器。
- ② 在 OCS 服务器上安装 OCS 2007 标准版，仅安装“主服务器”。
- ③ 在 OCS 服务器上创建域用户账户，并设置具体的电子邮件地址。
- ④ 在 OCS 服务器上安装 Web 客户端程序。
- ⑤ 在网络中已加入域的客户端计算机上，安装 OCS 2007 客户端。
- ⑥ 在网络中没有加入域的计算机上，或者其他能通过网络访问 OCS 2007 服务器的计算机上，

使用 Web 客户端。

- ⑦ 在能通过网络访问到 OCS 2007 服务器的智能手机上，安装智能手机客户端程序。

提示

如果网络规模比较小，Active Directory 和 OCS 可以部署在同一台服务器上。

2. 远程访问的网络架构

通常情况下，在带有远程访问用户的网络中，需要有两台计算机安装 OCS 2007，其中一台在企业网络内部充当“主服务器”，另一台在网络边缘充当访问代理服务器。

- ① 将 Windows Server 2003 服务器升级到 Active Directory。
- ② 将 OCS 主服务器加入域，同时提升为其额外域控制器。
- ③ 在 OCS 代理服务器上信任证书服务器上的证书颁发机构，并申请和安装证书。
- ④ 在 OCS 代理服务器上安装访问代理服务器。

3. 企业联盟用户网络架构

OCS 2007 SP1 还可以在两个或多个企业之间，使用“联盟”方式部署，从而让不同企业用户之间使用 Messenger 进行互相交流。这种部署方式是在“带有远程访问用户的网络”的基础上配置而来的。

4. 从 PC 到 PSTN 网络的访问

OCS 2007 还可以通过 SIP 到 PSTN 的网关，支持从 PC 到固定电话网络的通信。在 IP 电话流行的今天，OCS 2007 为用户提供了 IP 电话功能。如果可以租到价格低廉的包月长途线路，可以极大地节省企业的通信费用。

23.2 OCS 2007 需求

OCS 2007 服务器对服务器的软件和硬件都有一定的要求。如果只部署即时消息服务器，OCS 2007 对硬件的要求并不高。但是，如果需要部署存档服务器，则要求使用存取速度比较快的硬盘。

23.2.1 OCS 2007 的硬件要求

OCS 2007 服务器的最低配置要求如表 23-1 所示。

表 23-1 OCS 2007 的硬件要求

硬件组件	最低要求
CPU	Pentium III CPU，至少速度为 550 MHz；
网络适配器	10 Mbps
RAM	256 MB
硬盘驱动器	20 GB 硬盘

Microsoft 公司推荐的 OCS 2007 服务器最低配置要求如表 23-2 所示。

表 23-2 Microsoft 公司推荐的 OCS 的最低硬件要求

硬件组件	最低要求
CPU	双 x86 处理器，1.4 GHz
网络适配器	1 Gb/秒
RAM	2 GB
硬盘驱动器	2 x 36.4 GB Ultra2 SCSI，RAID 0 配置

此配置代表服务器级计算机的低端配置，如果使用更高配置的计算机，则可以获得更好的服务性能。建议用户为服务器准备两个硬盘驱动器，其中一个专用于写入 Office Communications 数据文件，另一个专门用于写入 Office Communications 日志文件。因为，MSDE 不能向位于同一硬盘驱动器的两个文件执行并行的写操作，建议将数据和日志文件分别存储在不同的硬盘驱动器上。

23.2.2 OCS 2007 支持的操作系统及环境需求

OCS 2007 支持的操作系统包括：

Windows Server 2003 标准版

Windows Server 2003 企业版

Windows Server 2003 数据中心版

安装 OCS 2007 的计算机，必需具备如下软件及网络环境：

Active Directory（Windows Server 2003 或）

公钥基础结构（PKI）

OCS 2007 的客户端软件是 Microsoft Windows Messenger 5.0，可以安装在以下系统平台上：

Windows Server 2003 标准版

Windows Server 2003 企业版

Windows Server 2003 R2 的各个版本

Windows XP Home Edition

Windows XP Professional

Windows 2000 Professional 带 Service Pack 3(SP3)

Windows 2000 Server 带 SP3

Windows 2000 Advanced Server 带 SP3

23.2.3 Windows 服务依赖项

为了确保服务器的安全，建议在安装 OCS 2007 服务器的计算机上禁用不需要的 Windows 服务。表 23-3 介绍 OCS 2007 所需的 Windows 服务，未列出的服务则可以将其禁用。

表 23-3 Office Communications Server 服务依赖项

OCS 2007 服务名称	Windows 服务依赖项
Office Communications Server 前端 (RTCSRV)	HTTP SSL (HTTP、IIS 管理服务、远程过程调用、安全账户管理器) Windows Management Instrumentation (事件日志和远程过程调用) Windows Management Instrumentation 驱动程序扩展 如果启用存档，消息队列 (消息队列访问控制、NTLM 安全支持提供程序、远程过程调用、RMCAST (Pgm) 协议驱动程序、TCP/IP 协议驱动程序、IPSEC 驱动程序、安全账户管理器)
Office Communications Server 音频/视频会议 (RTCAVMCU)	HTTP SSL (HTTP、IIS 管理服务、远程过程调用、安全账户管理器) Windows Management Instrumentation (事件日志和远程过程调用)
Office Communications Server IM 会议 (RTCIMMCU)	HTTP SSL (HTTP、IIS 管理服务、远程过程调用、安全账户管理器) Windows Management Instrumentation (事件日志和远程过程调用)
Office Communications Server 电话会议 (RTCACPMCU)	HTTP SSL (HTTP、IIS 管理服务、远程过程调用、安全账户管理器) Windows Management Instrumentation (事件日志和远程过程调用)
Office Communications Server Web 会议 (RTCDATAMCU)	HTTP SSL (HTTP、IIS 管理服务、远程过程调用、安全账户管理器) Windows Management Instrumentation (远程过程调用)
Office Communications Server 存档和 CDR (RTCLOG)	消息队列 (消息队列访问控制、NTLM 安全支持提供程序、远程过程调用、RMCAST (Pgm) 协议驱动程序、TCP/IP 协议驱动程序、IPSEC 驱动程序、安全账户管理器)
Office Communications Server 音频/视频身份验证 (RTCMRAUTH)	Windows Management Instrumentation (事件日志和远程过程调用)
Office Communications Server 音频/视频边缘 (RTCMEDIARELAY)	Office Communications Server 音频/视频身份验证 Windows Management Instrumentation (事件日志和远程过程调用)
Office Communications Server 访问边缘 (RTCSRV)	Windows Management Instrumentation (事件日志和远程过程调用) Windows Management Instrumentation 驱动程序扩展
Office Communications Server Web 会议边缘 (RTCDATAPROXY)	Windows Management Instrumentation (事件日志和远程过程调用)
Office Communications Server 中介 (RTCMEDSRV)	Windows Management Instrumentation (远程过程调用)

23.3 部署 OCS 2007

在中小规模的企业网络中，使用 OCS 2007 标准版就已经足够了。通常需要两台服务器，其中一台部署 Active Directory，提供 OCS 所需的网络环境，另一台服务器直接安装 OCS 2007。

23.3.1 设置 IP 地址

① 将 Windows Server 2003 服务器升级到 Active Directory，并命名为 AD-Server，IP 地址为 162.168.80.10，子网掩码为 255.255.255.0，DNS 地址为 127.0.0.1，域名为 msft.com，如图 23-1 所示。

② 将 OCS 服务器升级到域的额外域控制器，计算机名称为 OCS 2007，IP 地址为 162.168.80.20，设置 DNS 地址为域控制器地址 162.168.80.10，如图 23-2 所示。

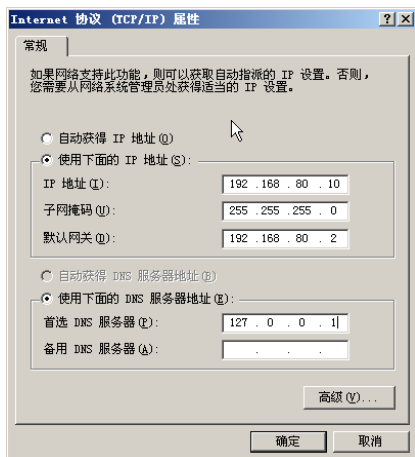


图 23-1 域控制器 IP 地址

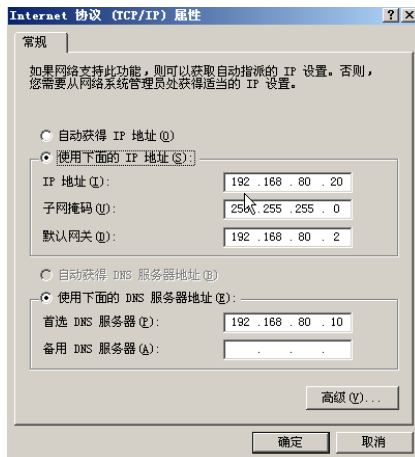


图 23-2 OCS 服务器地址

- ③ 在域控制器上部署 OCS 2007 架构。
- ④ 在 OCS 服务器上安装 OCS 2007。
- ⑤ 在 Active Directory 中创建用户账户，同时为 SIP 启用用户账户。
- ⑥ 网络中的任意工作站上安装 OCS 2007 客户端。

23.3.2 在域控制器上准备 OCS 架构

在域控制器上，以管理员账户登录，将 OCS 2007 标准版安装光盘放在光驱中，运行 Office Communications Server 2007 安装程序，以准备 OCS 架构。

1. 准备 Active Directory

如果域控制器上没有安装 Microsoft Visual C++ 2005 SP1，则运行 OCS 2007 光盘时会显示如图 23-3 所示对话框，要求安装所需组件，单击“是”按钮即可。在“欢迎部署 Office Communications Server 2007 Standard Edition Server”对话框中，单击“部署 Standard Edition Server(s)”链接，显示如图 23-4 所示“部署 Standard Edition Server”对话框。

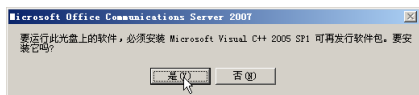


图 23-3 安装 SP1



图 23-4 部署 Standard Edition Server

- ① 单击“准备 Active Directory”链接，显示如图 23-5 所示“为 Office Communications Server 准备 Active Directory”对话框。
- ② 单击“运行”按钮，显示如图 23-6 所示“Active Directory 架构准备向导”对话框。
- ③ 单击“下一步”按钮，显示如图 23-7 所示“架构文件的目录位置”对话框，选择“默认：架构文件与安装程序位于同一目录中”单选按钮。



图 23-5 准备 Active Directory



图 23-6 欢迎使用 Active Directory 准备

- ④ 单击“下一步”按钮，显示如图 23-8 所示“已准备好进行架构准备”对话框。

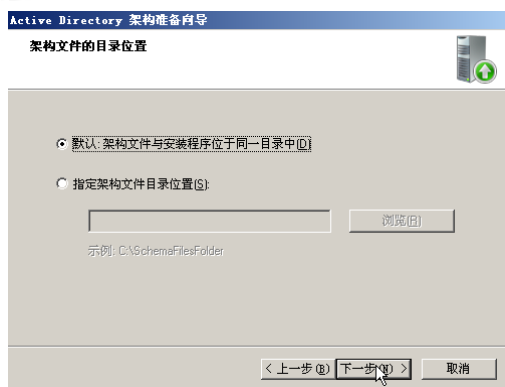


图 23-7 架构文件的目录位置

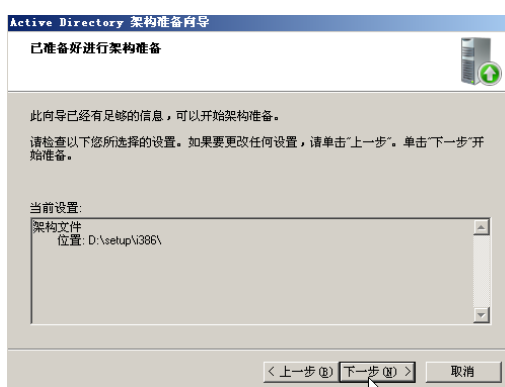


图 23-8 已准备好架构准备

- ⑤ 单击“下一步”按钮，安装向导开始为 OCS 2007 准备所需的 Active Directory 架构。完成后，显示如图 23-9 所示“‘架构准备向导’已成功完成”对话框。

- ⑥ 单击“完成”按钮，返回部署 Standard Edition Server，如图 23-10 所示。准备架构已显示为“完成”状态。

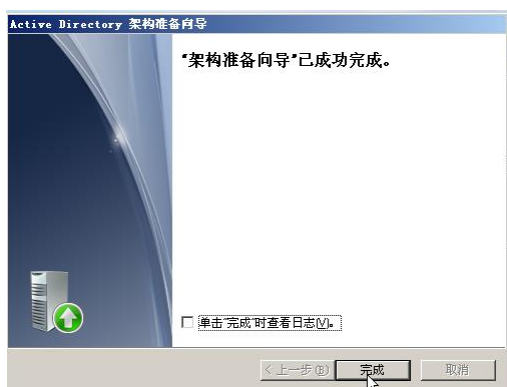


图 23-9 “架构准备向导”已完成



图 23-10 准备 Active Directory 架构完成

2. 验证架构分区的复制

- (1) 将 OCS 光盘放入光驱，并打开命令提示符窗口。定位到光盘中的\Setup\I386 目录下，输入如下命令：

```
LcsCmd /Forest /action:CheckSchemaPrepState /PDCRequired:FALSE
```

执行该命令后，显示如图 23-11 所示结果。

(2) 打开由该命令创建的 HTML 日志文件，显示如图 23-12 所示“Office Communications Server 2007 部署日志”窗口。单击“执行操作”选项，验证“架构准备状态”的结果是否为当前已经安装的服务器的版本，以及“执行结果”是否显示“成功”状态。

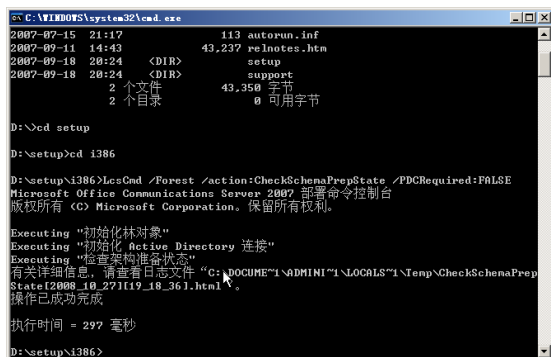


图 23-11 验证架构分区的复制



图 23-12 OCS 2007 部署日志

3. 准备林

① 在“为 Office Communications Server 准备 Active Directory”对话框中，单击“准备林”选项区域的“运行”按钮，显示如图 23-13 所示“欢迎使用‘林准备向导’”对话框。

② 单击“下一步”按钮继续，显示如图 23-14 所示“选择用于存储全局设置的位置”对话框，选择“根目录域中的系统容器”单选按钮。

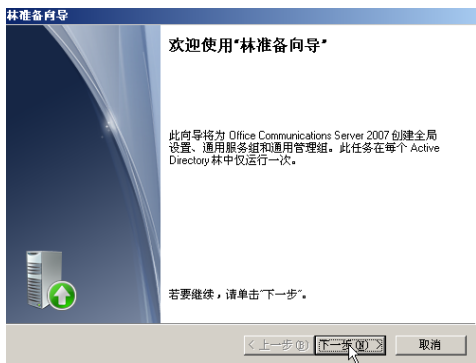


图 23-13 林准备向导

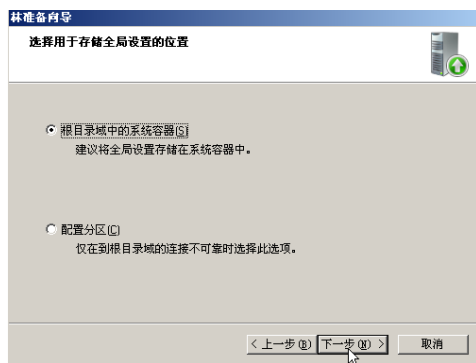


图 23-14 选择用于存储全局设置的位置

③ 单击“下一步”按钮，显示如图 23-15 所示“通用组的位置”对话框，在“域”下拉列表中选择“msft.com”选项。

④ 单击“下一步”按钮，显示“选择默认路由的 sip 域”对话框，按照默认值即可。单击“下一步”按钮，显示如图 23-16 所示“‘林准备向导’已成功完成”对话框。

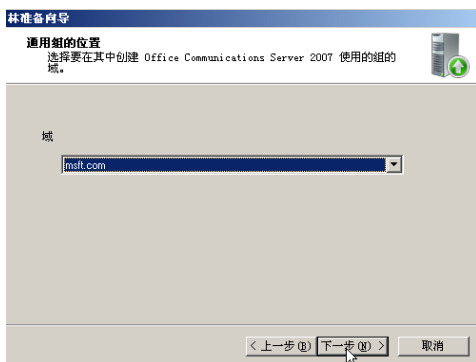


图 23-15 通用组的位置



图 23-16 完成林准备向导

⑤ 单击“完成”按钮，保存设置即可。

4. 验证全局设置和全局目录的设置

① 将 Microsoft Office Communications Server 光盘放入光驱，打开命令提示符窗口，转到安装光盘的\Setup\I386 目录下，输入如下命令（如图 23-17 所示）：

```
LcsCmd /forest /action:CheckForestPrepState /PDCRequired:FALSE
```

② 执行命令后，显示如图 23-18 所示结果。

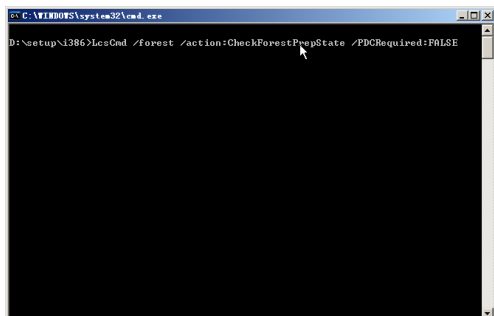


图 23-17 命令提示符窗口

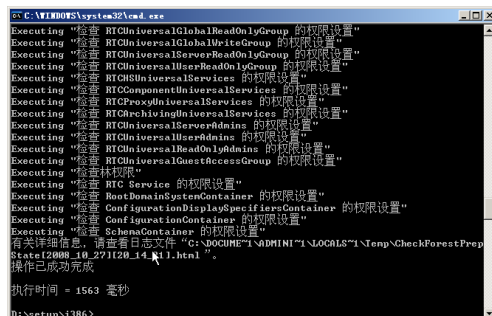


图 23-18 操作完成

③ 打开该命令创建的 HTML 日志文件，如图 23-19 所示，检查验证结果是否显示为“林设置：就绪”，以及“执行结果”列下面是否出现“成功”。



图 23-19 检查验证结果

5. 准备当前域

① 在“为 Office Communications Server 准备 Active Directory”对话框中，单击“准备当前域”选项区域的“运行”按钮，显示如图 23-20 所示的“欢迎使用‘域准备向导’”对话框。

② 单击“下一步”按钮，显示如图 23-21 所示的“域准备信息”对话框。

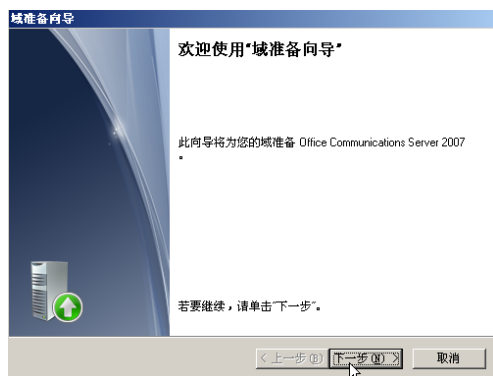


图 23-20 域准备向导



图 23-21 域准备信息

- ③ 单击“下一步”按钮，显示如图 23-22 所示的“已准备好进行域准备”对话框。
- ④ 单击“下一步”按钮，开始进行域准备。完成之后显示如图 23-23 所示的“‘域准备向导’已成功完成”对话框。



图 23-22 已准备好进行域准备



图 23-23 成功完成

- ⑤ 单击“完成”按钮，退出即可。

23.3.3 部署 OCS 2007

安装 OCS 2007 之前，必须确保已经加入到域，并且提升为额外域控制器。使用域管理员账户登录到域控制器，即可开始相关的准备工作。

1. 安装证书服务

OCS 2007 服务器需要使用证书颁发机构，对于中小规模的网络而言，可以在 OCS 2007 服务器上同时部署 CA，如果网络规模较大，建议分配专用的 CA 服务器。

① 将 Windows Server 2003 安装光盘放入光驱，打开“添加或删除程序”窗口，单击“添加或删除 Windows 组件”按钮，显示如图 23-24 所示的“Windows 组件向导”对话框，在“组件”列表中选“证书服务”复选框。

② 单击“下一步”按钮，显示如图 23-25 所示的“CA 类型”对话框，选择“独立根 CA”单选按钮。

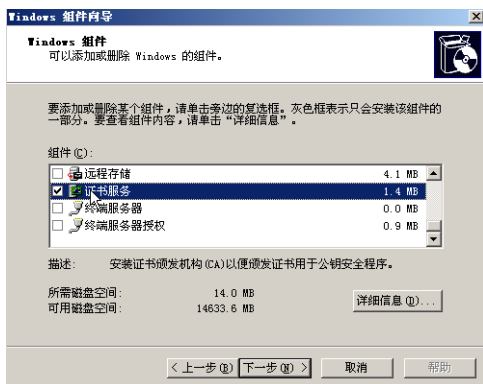


图 23-24 Windows 组件向导

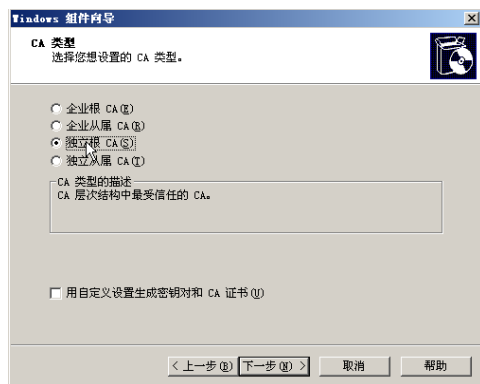


图 23-25 CA 类型

③ 单击“下一步”按钮，显示如图 23-26 所示的“CA 识别信息”对话框，在“此 CA 的公用名称”文本框中，输入 heuet.org。

④ 单击“下一步”按钮，显示如图 23-27 所示的“证书数据库设置”对话框，保持默认值即可。单击“下一步”按钮，证书服务安装完成。



图 23-26 CA 识别信息

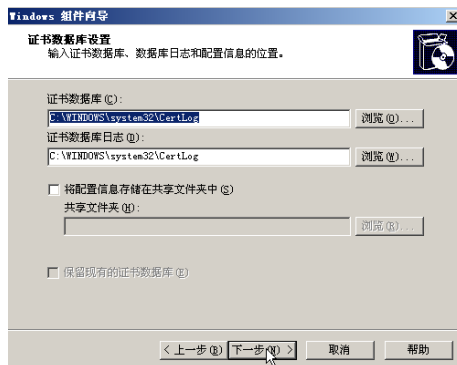


图 23-27 证书数据库设置



域功能级别必须为 Windows Server 2003，否则无法部署。

2. 部署 Standard Edition Server

将 OCS 2007 标准版安装光盘放在光驱，运行 OCS 2007 安装程序，显示如图 23-28 所示的“Office Communications Server 2007 Standard Edition”对话框。单击“部署 Standard Edition Server”链接，显示如图 23-29 所示“部署 Standard Edition Server”对话框。



图 23-28 OCS 2007 安装程序



图 23-29 部署 Standard Edition Server

(1) 部署服务器

- ① 在“部署服务器”选项区域，单击“运行”按钮，显示如图 23-30 所示的“欢迎使用‘部署服务器向导’”对话框。
- ② 单击“下一步”按钮，显示如图 23-31 所示的“许可协议”对话框，选择“我接受许可协议中的条款”单选按钮。

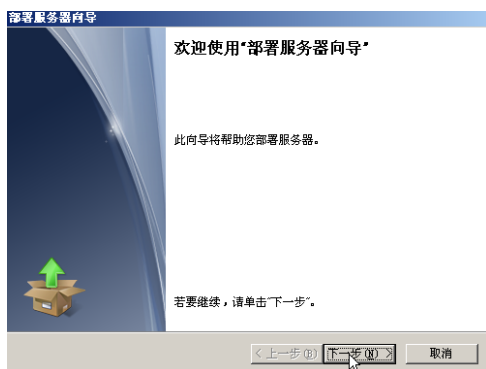


图 23-30 部署服务器向导



图 23-31 许可协议

③ 单击“下一步”按钮，显示如图 23-32 所示的“服务器文件的位置”对话框，单击“浏览”按钮，可以重新选择安装文件夹的路径。

④ 单击“下一步”按钮，显示如图 23-33 所示的“Standard Edition Server 的主要服务账户”对话框，选择“创建新账户”单选按钮，在“账户名”文本框中，输入系统默认用户名 RTCService，在“密码”和“确认密码”文本框中，键入为新建用户设置的密码。



图 23-32 服务器文件的位置

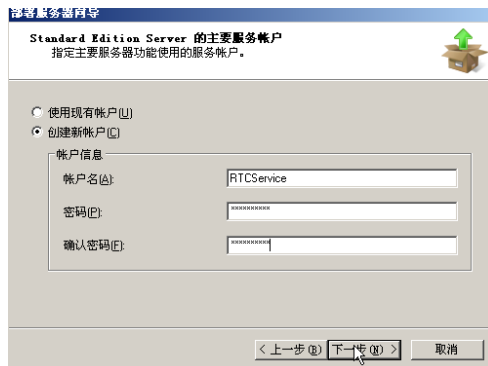


图 23-33 Standard Edition Server 的主要服务帐户

⑤ 单击“下一步”按钮，显示如图 23-34 所示的“此 Standard Edition Server 的组件服务账户”对话框，选择“创建新账户”单选按钮，在“账户名”文本框中，输入系统默认用户名 RTCComponentService，在“密码”和“确认密码”文本框中键入为新用户设置的密码。

⑥ 单击“下一步”按钮，显示如图 23-35 所示的“Web 场 FQDN”对话框，按照默认值即可。

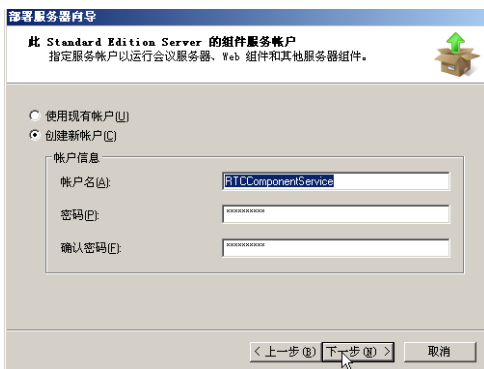


图 23-34 指定组件账户

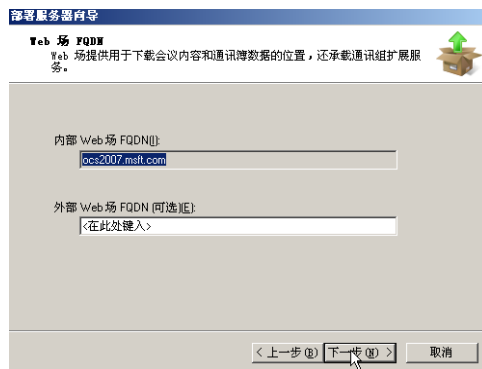


图 23-35 Web 场 FQDN

⑦ 单击“下一步”按钮，显示如图 23-36 所示的“数据库文件的位置”对话框，可以重新选择安装位置，也可以使用默认设置。

⑧ 单击“下一步”按钮，显示如图 23-37 所示的“已准备好部署服务器”对话框。

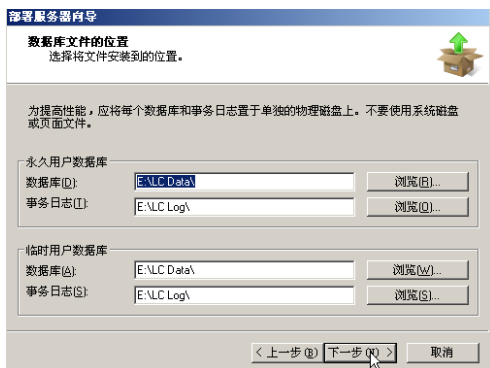


图 23-36 选择位置

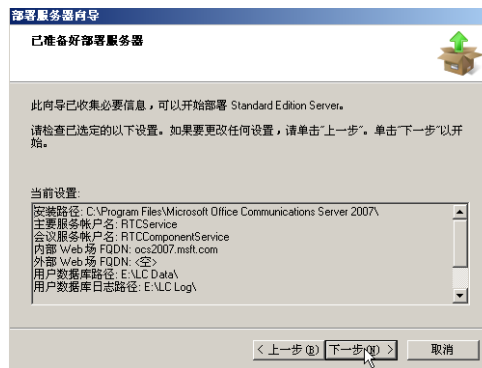


图 23-37 查看选项

⑨ 单击“下一步”按钮，开始部署 Standard Edition Server。部署完成后，显示如图 23-38 所示的“部署服务器向导”已成功完成”对话框。

⑩ 单击“完成”按钮，返回到“部署 Standard Edition Server”对话框，如图 23-39 所示。

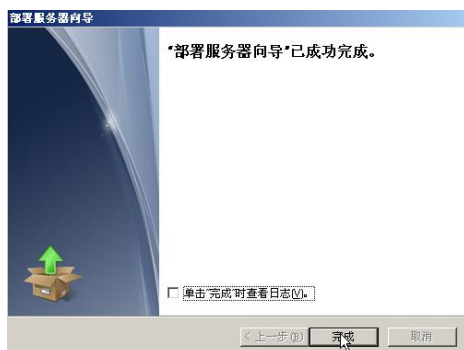


图 23-38 完成部署服务器向导



图 23-39 部署 Standard Edition Server

(2) 配置服务器

① 在“部署 Standard Edition Server”对话框的“配置服务器”选项区域中，单击“运行”按钮，显示如图 23-40 所示的“欢迎使用‘配置池/服务器向导’”对话框。

② 单击“下一步”按钮，显示如图 23-41 所示的“要配置的服务器或池”对话框，选择下拉列表中的“ocs2007.msft.com”选项。

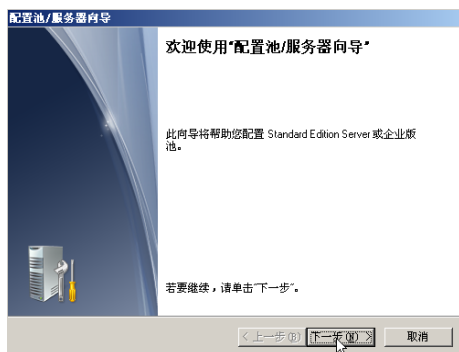


图 23-40 配置池/服务器向导

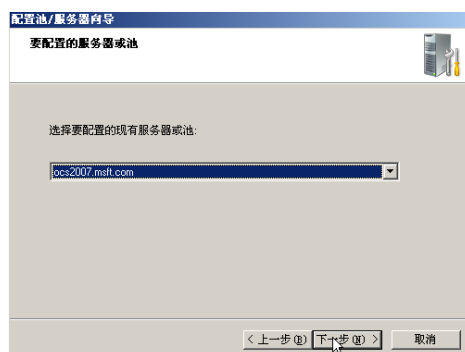


图 23-41 选择服务器或池

③ 单击“下一步”按钮，显示如图 23-42 所示的“SIP 域”对话框，保持默认值即可。

④ 单击“下一步”按钮，显示如图 23-43 所示的“客户端登录设置”对话框，选择“部分或所有客户端使用 DNS SRV 记录进行自动登录”单选按钮，选中“使用此服务器或池验证并重定向自动客户端登录请求”复选框。



图 23-42 SIP 域

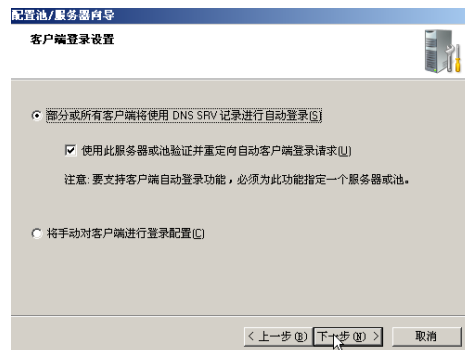


图 23-43 客户端登录设置

⑤ 单击“下一步”按钮，显示如图 23-44 所示的“用于自动登录的 SIP 域”对话框，选中域 msft.com

选项。

⑥ 单击“下一步”按钮，显示如图 23-45 所示的“外部用户访问配置”对话框，选择“现在不要针对外部用户访问进行配置”单选按钮。



图 23-44 用于自动登录的 SIP 域

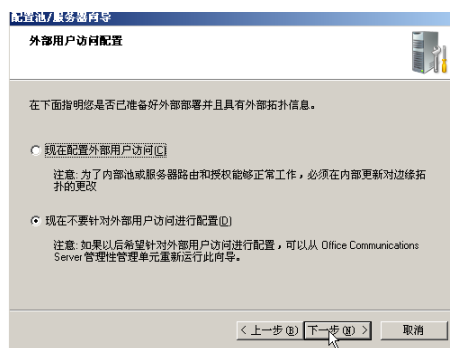


图 23-45 外部用户访问配置

⑦ 单击“下一步”按钮，显示如图 23-46 所示的“已准备好配置服务器或池”对话框。

⑧ 单击“下一步”按钮，开始配置。完成后，显示如图 23-47 所示““配置服务器或池向导”已成功完成”对话框。



图 23-46 已准备的配置信息



图 23-47 完成“配置服务器或池向导”

⑨ 单击“完成”按钮，关闭向导。

(3) 配置证书

① 在“部署 Standard Edition Server”对话框的“配置证书”选项区域中，单击“运行”按钮，显示“欢迎使用‘证书向导’”对话框。单击“下一步”按钮，显示如图 23-48 所示的“可用的证书任务”对话框，选择“创建新的证书”单选按钮。

② 单击“下一步”按钮，显示如图 23-49 所示的“延迟的请求或即时请求”对话框，选择“立即请求发送联机证书颁发机构”单选按钮。



图 23-48 可用的证书服务

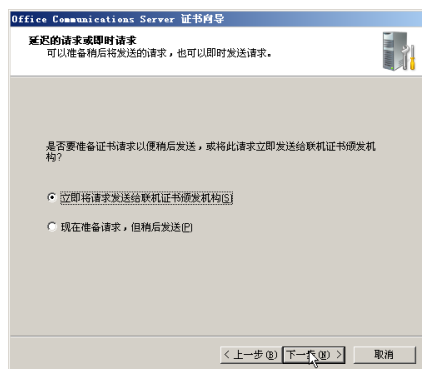


图 23-49 延迟的请求或即时请求

- ③ 单击“下一步”按钮，显示如图 23-50 所示的“名称和安全设置”对话框，保持默认值即可。
- ④ 单击“下一步”按钮，显示如图 23-51 所示的“组织信息”对话框，选择相应的“组织”和“组织单位”即可。

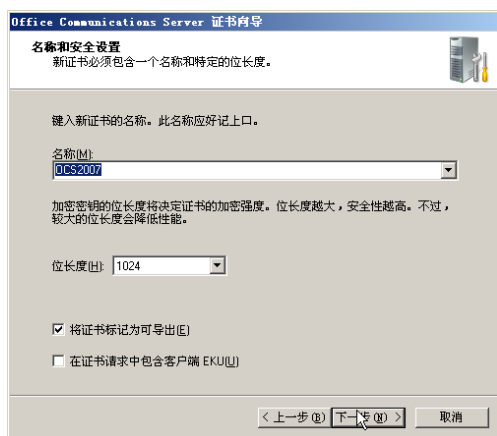


图 23-50 名称和安全设置



图 23-51 组织信息

- ⑤ 单击“下一步”按钮，显示如图 23-52 所示的“服务器的使用者名称”对话框，保持默认值即可。
- ⑥ 单击“下一步”按钮，显示如图 23-53 所示的“地理信息”对话框，输入对应的“国家/地区”、“州/省”和“市/县”等信息。

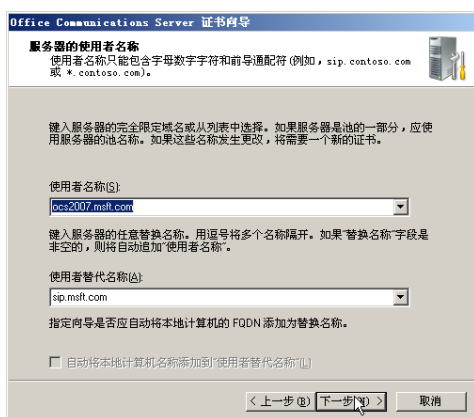


图 23-52 服务器的使用者名称

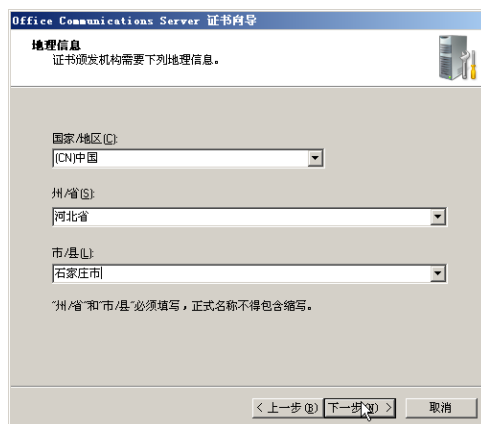


图 23-53 地理信息

- ⑦ 单击“下一步”按钮，显示如图 23-54 所示的“选择证书颁发机构”对话框，保持默认值即可。
- ⑧ 单击“下一步”按钮，显示如图 23-55 所示的“请求摘要”对话框，检查配置信息是否正确。



图 23-54 选择颁发机构



图 23-55 查看请求摘要

⑨ 单击“下一步”按钮，配置向导完成，显示如图 23-56 所示的“‘证书向导’已成功完成”对话框。单击“完成”按钮，关闭向导。

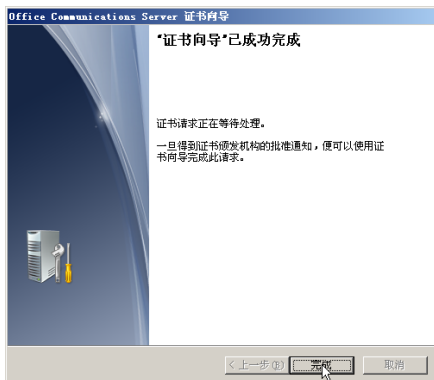


图 23-56 完成证书向导

⑩ 依次单击“开始”→“程序”→“管理工具”→“证书颁发机构”选项，显示如图 23-57 所示的“证书颁发机构”窗口。展开“挂起的申请”选项，右击“证书”并依次选择“所有任务”→“颁发”选项，向 OCS 服务器颁发证书。

⑪ 返回到“部署 Standard Edition Server”向导，再次在“配置证书”选项区域中，单击“运行”按钮，显示如图 23-58 所示的“欢迎使用‘证书向导’”对话框。

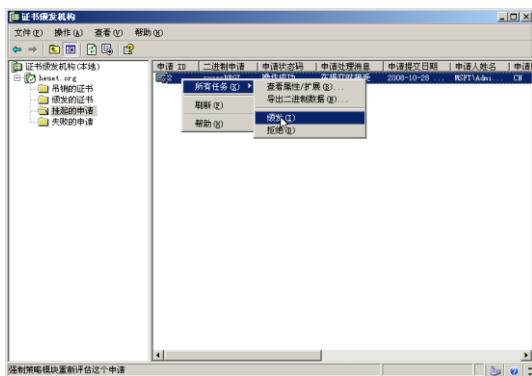


图 23-57 证书颁发机构

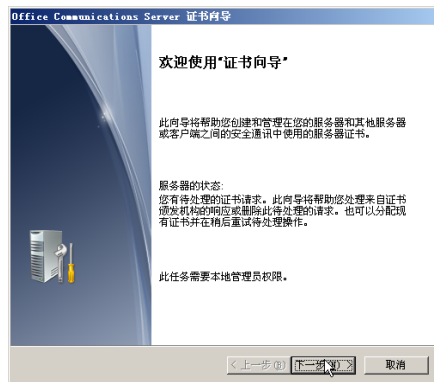


图 23-58 欢迎使用“证书向导”

⑫ 单击“下一步”按钮，显示如图 23-59 所示的“待处理的证书请求”对话框，选择“处理待处理的请求并导入证书”单选按钮。

⑬ 单击“下一步”按钮，显示如图 23-60 所示的“待处理的证书请求”对话框，提示确认是否为所选对象，保持默认值即可。



图 23-59 待处理的证书请求

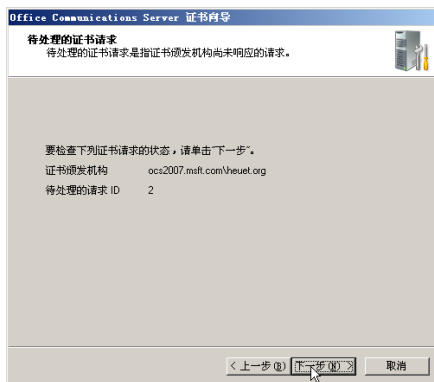


图 23-60 待处理的证书请求

- ⑭ 单击“下一步”按钮，显示如图 23-61 所示的“‘证书向导’已成功完成”对话框。
- ⑮ 单击“分配”按钮，显示如图 23-62 所示的“Office Communications Server 证书向导”对话框，证书分配成功。

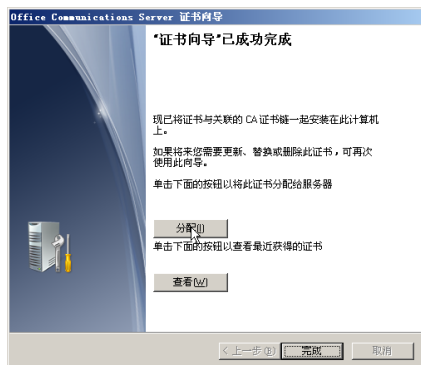


图 23-61 分配证书



图 23-62 证书完成

- ⑯ 单击“确定”按钮，关闭向导。
- (4) 配置 Web 组件证书
 - ① 依次单击“开始”→“程序”→“管理工具”→“Internet 信息服务”选项，显示“Internet 信息服务管理器”窗口。右击“默认网站”选择快捷菜单中的“属性”选项，显示“默认网站 属性”对话框，切换到如图 23-63 所示的“目录安全性”选项卡。
 - ② 单击“服务器证书”按钮，显示如图 23-64 所示的“欢迎使用 Web 服务器证书向导”对话框。

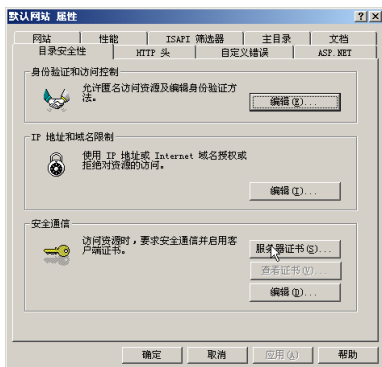


图 23-63 打开服务器证书

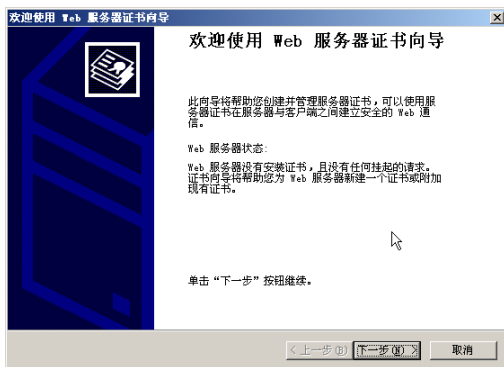


图 23-64 进入向导

- ③ 单击“下一步”按钮，显示如图 23-65 所示的“服务器证书”对话框，选择“分配现有证书”单选按钮。
- ④ 单击“下一步”按钮，显示如图 23-66 所示的“可用证书”对话框，选择上述操作过程中，从证书服务器获得的证书即可。

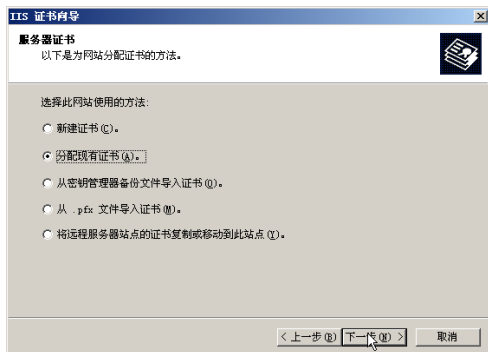


图 23-65 服务器证书

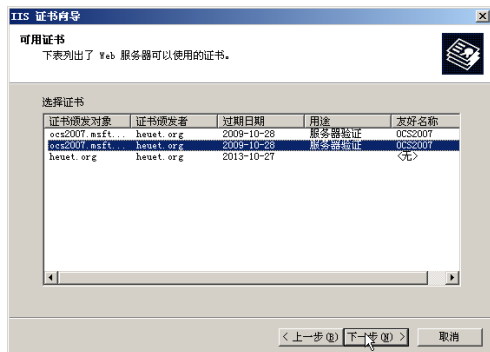


图 23-66 可用证书

- ⑤ 单击“下一步”按钮，显示如图 23-67 所示的“SSL 端口”对话框，保持默认端口。
- ⑥ 单击“下一步”按钮，显示如图 23-68 所示的“证书摘要”对话框，查看证书信息是否正确。



图 23-67 选择端口

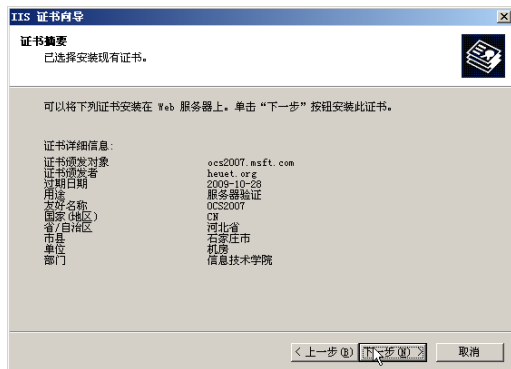


图 23-68 证书摘要

- ⑦ 单击“下一步”按钮，显示如图 23-69 所示的“完成 Web 服务器证书向导”对话框。

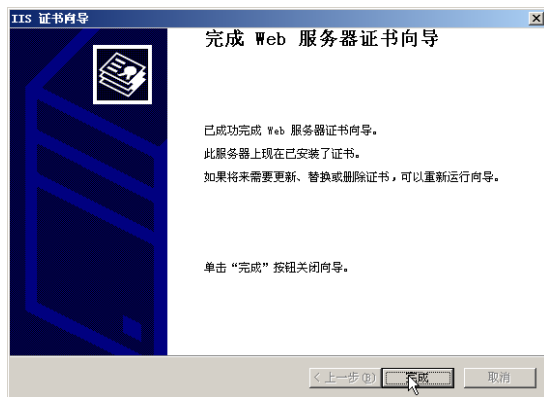


图 23-69 完成 Web 服务器证书向导

- ⑧ 单击“完成”按钮，关闭向导。

(5) 验证复制

- ① 将 OCS 2007 标准版安装光盘放在光驱中。打开命令提示符窗口，转到安装光盘的\Setup\I386 目录下，输入如下命令（如图 23-70 所示）：

```
LcsCmd /server /action:CheckLCServerState /role:se /PDCRequired:FALSE
```

- ② 成功执行后，显示如图 23-71 所示的结果。

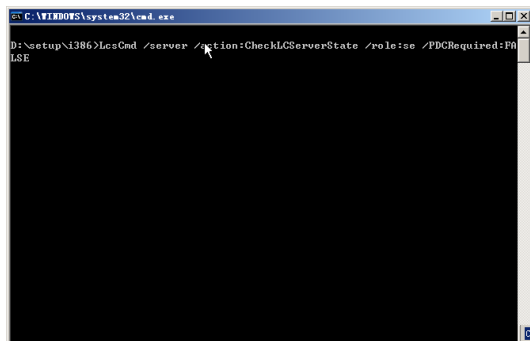


图 23-70 输入命令

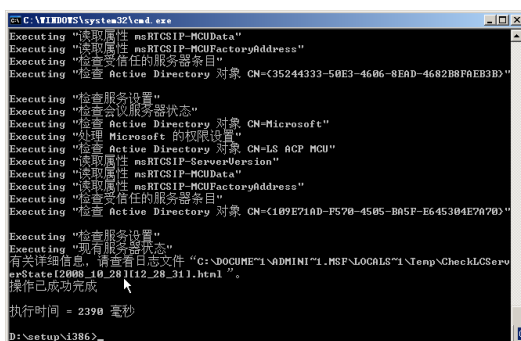


图 23-71 操作成功

- ③ 打开该命令所创建的 HTML 日志文件，如图 23-72 所示。检查各项信息的复制结果是否为“成功”状态。



图 23-72 复制成功

(6) 启动服务

① 在“部署 Standard Edition Server”对话框的“启动服务”选项区域中，单击“运行”按钮，显示如图 23-73 所示“欢迎使用‘启动服务向导’”对话框。

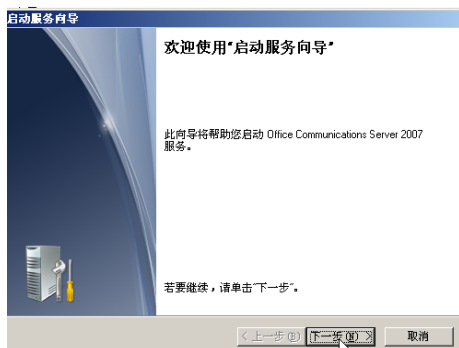


图 23-73 欢迎使用“启动服务向导”

② 单击“下一步”按钮，显示如图 23-74 所示“启动 Office Communications Service 2007 服务”对话框。

③ 单击“下一步”按钮，即可启动相应服务。完成后，显示如图 23-75 所示“‘启动服务向导’已成功完成”对话框。

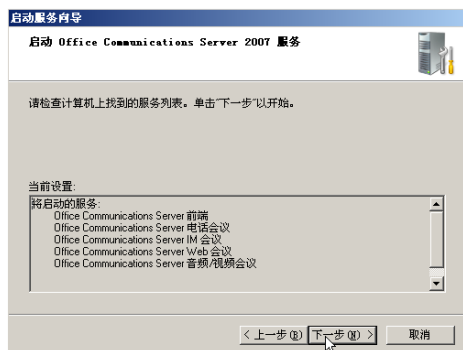


图 23-74 启动 OCS 2007 服务



图 23-75 完成启动服务向导

23.3.4 在 OCS 服务器上配置 TCP

在 OCS 2007 服务器上配置了证书后，使用以下步骤在 OCS 上配置 TCP。

① 依次选择“开始”→“程序”→“管理工具”→“Office Communications Server 2007”选项，启动 OCS 2007。依次展开“林”→“Stander Edition 服务器”→“OCS 2007”→“ocs 2007.msft.com”选项，如图 23-76 所示。

② 右击“ocs 2007.msft.com”选项，依次选择快捷菜单中“属性”→“前端属性”选项，显示如图 23-77 所示的“前端服务器属性”对话框。

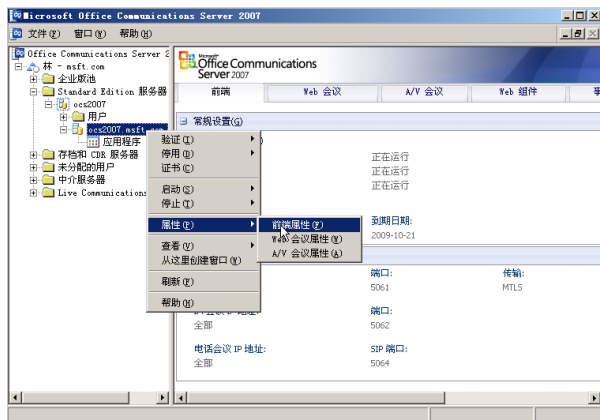


图 23-76 OCS 2007

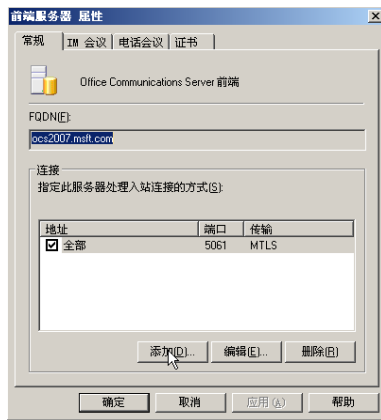


图 23-77 前端服务器 属性

③ 在“常规”选项卡中单击“添加”按钮，显示如图 23-78 所示的“添加连接”对话框，在“传输”下拉列表中选择“TCP”选项，其他选项保持默认设置即可。

④ 单击“确定”按钮返回“常规”选项卡，TCP 连接已被添加到列表中，如图 23-79 所示。

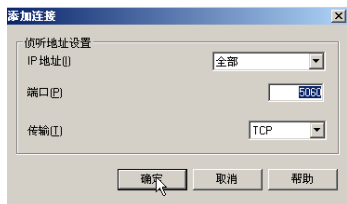


图 23-78 添加连接

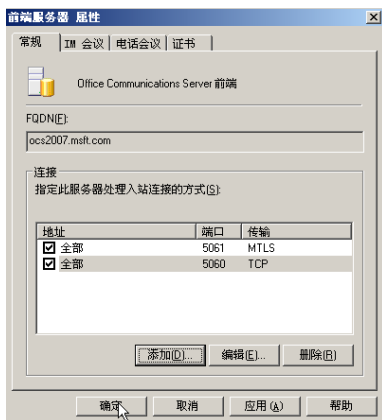


图 23-79 添加 TCP 连接完成

⑤ 单击“确定”按钮，保存设置，返回 OCS 2007 主窗口。右击“林-msft.com”并依次选择快捷菜单中的“属性”→“全局属性”选项，显示如图 23-80 所示的“Office Communications Server 全局属性”对话框。切换到“会议”选项卡，在“匿名参与者”下拉列表中，选择“允许用户邀请匿名参与者”选项；在“全局策略”下拉列表中，选择“Policy 4 (Medium Low)”选项。

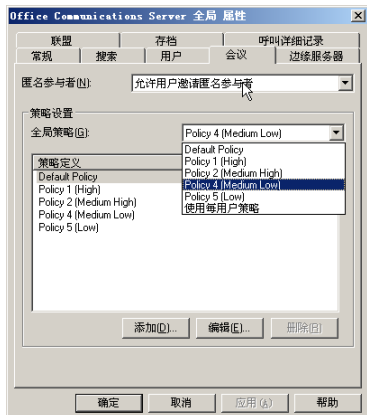


图 23-80 Office Communications Server 全局属性

⑥ 单击“确定”按钮，保存设置。

23.3.5 创建域用户

由于已经将 OCS 2007 服务器配置当前域的额外域控制器，以管理员账户登录域控制器或 OCS 服务器均可完成域用户账户的创建。为了便于网络管理，建议为 OCS 2007 客户端配置单独的组织单位，并在该 OU 中创建用户账户。例如，本例中创建的 3 个用户账户分别为 ocs1、ocs2、ocs3，其对应的电子邮箱地址分别为 ocs1@msft.com、ocs2@msft.com、ocs3@msft.com。

如果系统中有 Exchange，并且创建用户的过程中已经指定了邮箱地址，则无需再单独配置。

23.3.6 配置 OCS 的用户账户

默认情况下，域用户账户的 OCS 功能并未启用。管理员可以通过“Active Directory 用户和计算机”管理工具，为一个或一批用户启用 OCS 功能。

在 OCS 2007 服务器上，打开“Active Directory 用户和计算机”控制台，右击希望配置的用户账户（以 OCS1 为例），选择快捷菜单中的“属性”按钮，显示如图 23-81 所示的“ocs1 属性”对话框。

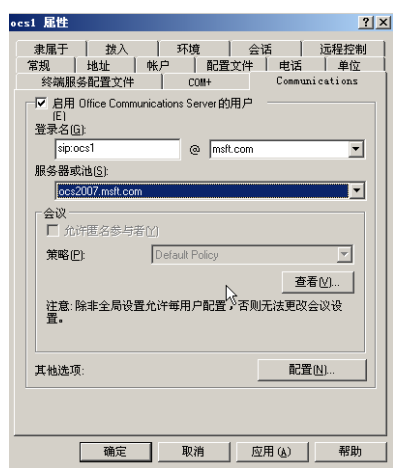


图 23-81 Communications

切换到“Communications”选项卡，选中“启用 office Communications 的用户”复选框。在“登录名”文本框中，输入 sip:ocs1。在“服务器或池”下拉列表中，选择 OCS 服务器的名称，即 ocs2007.msft.com。单击“确定”按钮保存设置。

按照如下方法，管理员可以为一批用户同时启用 Office Communications 功能，但必须确保所选用都已经配置有效的电子邮件地址。

① 在“Active Directory 用户和计算机”窗口中，同时选中所有需要配置 OCS 客户端的用户账户，右击并选择快捷菜单中的“所有任务”→“为 Office Communications 启用用户”选项，启动“启用 Office Communications Server 用户向导”。

② 单击“下一步”按钮，显示如图 23-82 所示的“选择服务器或池”对话框，选择下拉菜单中选择 OCS 服务器。

③ 单击“下一步”按钮，显示如图 23-83 所示的“启用操作状态”对话框。

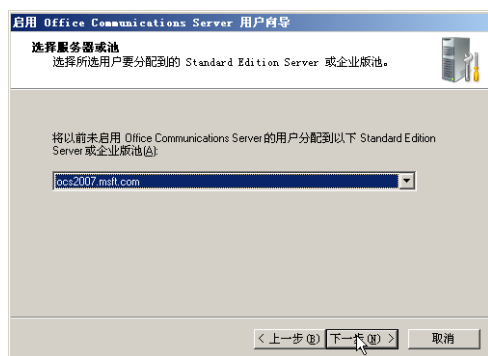


图 23-82 选择服务器或池



图 23-83 启用操作状态

④ 单击“完成”按钮，关闭向导。

23.4 OCS 2007 客户端

Office Communicator 2007 客户端，可以帮助用户使用包括即时消息（IM）、语音和视频在内的一

系列不同通信方式，方便地与不同位置或时区的其他用户通信，从而提高工作效率，可以与整个 Microsoft Office System 2007 中的所有组件配合使用。

►► 23.4.1 OCS 2007 客户端的新增功能

Office Communicator 2007 提供了一些新增功能，旨在改进用户查找同事及与同事建立联系的方式，可使联系人和联系人列表的管理变得更加轻松。

1. 联系人管理

Office Communicator 2007 在联系人和联系人列表管理方面提供了很多新增功能，使用户可以获得更有效的控制和更大的灵活性。Office Communicator 2007 还引入了新的状态，可以更准确地反映每个人进行沟通的能力和意愿。此外，Office Communicator 2007 还增强了即时消息的功能，包括支持在即时消息中使用 RTF 格式的文本。Office Communications Server 和 Office Communicator 2007 的所有配置都可以使用下列功能：

显示最近的联系人。Communicator 联系人列表中现在提供了“最近的联系人”组。“最近的联系人”组是包括最近 10 个与用户进行通信（通过 IM、电话或视频）的联系人列表。

将联系人拖放到组中。用户现在可以将联系人从“搜索结果”窗格拖动到联系人列表中。还可以在联系人列表中的各个组之间拖放联系人。需要注意的是，用户不能将联系人拖动到通信组中。

在联系人列表和“对话”窗口名单之间拖放联系人。通过将联系人从联系人列表拖动到“对话”窗口的名单中，可以将联系人添加到 IM、呼叫或视频会话中。也可以将联系人从“对话”窗口的名单拖动到联系人表中，从而将这些联系人添加到联系人列表中。

通信组集成。用户可以将 Active Directory 中所有启用邮件的组添加到联系人列表中。

改进的联系人详细信息用户界面。单击联系人的“状态”按钮可以查看其联系人卡片。联系人卡片可提供有关该联系人的其他详细信息，以及用于与此人进行联系的选项。

2. 增强的状态和状态管理

Office Communicator 2007 提供了新的状态，主要包括：

非活动。联系人可能有空，但该联系人的计算机处于空闲状态的时间已经超过空闲时间间隔（默认为 5 分钟）。

忙碌非活动。联系人正在参与其他活动，例如参加会议，但该联系人的计算机处于非活动状态的时间已经超过空闲时间间隔（默认为 5 分钟）。

转变状态。Office Communicator 2007 引入的新状态由用户可配置的空闲时间设置决定，该设置会监视用户在计算机上的活动。如果在用户的计算机上未检测到活动，则状态会从“空闲”转变为“非活动”，再转变为“离开”。

改进的状态管理。Office Communicator 2007 允许用户对状态信息访问权限进行更具体的控制。

用户可以为联系人分配不同的访问级别，来控制哪些联系人可以查看用户的状态信息，以及可以查看哪些信息。例如，可以为关系最亲密的同事分配“团队”访问级别，这将允许其查看用户的移动电话号码，并允许其在用户处于“请勿打扰”模式建立联系。对于公司中的其他同事，可以分配“公司”访问级别，这将允许他们查看用户的工作电话号码，但不允许查看用户的移动电话号码，而且不允许其在用户处于“请勿打扰”模式时建立联系。

优先列表。用户可以为联系人分配“团队”访问级别以创建优先联系人列表，即使用户设置为“请勿打扰”状态，这些优先联系人仍能与用户进行通信。

位置设置配置。用户可以从 Communicator 窗口状态区域中的“状态”菜单中，通过“住宅”或“办

公室”选项，设置自己的位置状态。已被授予“个人”或“团队”访问级别的联系人可以看到位置信息。

3. 会议

通过使用 Office Communicator 2007，会议功能已优化为支持多种通信模式，包括即时消息、音频、视频和数据共享。用户可以在各模式之间无缝转换，无需退出“对话”窗口或重新邀请用户。例如，用户可以将一对一的 IM 会话升级为多方电话会议，并通过 Live Meeting 添加数据共享，以共享其桌面上的幻灯片、文档或应用程序。Office Communicator 2007 中新增会议功能如下：

外拨到备用电话号码的功能。可以通过将会议邀请重定向到备用电话（如移动电话）来参加会议。

此外，如果用户是会议主持人，则可以通过外拨 PSTN/PBX 电话号码或移动电话号码来邀请用户参加会议。

一对一电话对话到会议呼叫的无缝切换。只需邀请新联系人加入会议呼叫，便可以将一对一电话对话无缝切换到会议呼叫。

通过在联系人窗口中选择组来开始会议呼叫的功能。可以在联系人列表中选择多个联系人或单击联系人列表中的组，然后选择某个会议呼叫选项来启动会议。

会议名单中改进的连接。会议名单中的新图标提供了更多的会议连接状态，指示用户的状态是“正在邀请”、“正在连接”还是“已连接”。

重新加入体验。如果用户从会议中断开，现在可以使用“重新加入”按钮轻松地重新加入会议。

4. 电话和视频

Office Communicator 2007 中新的电话和视频功能包括：

在各个模式之间无缝转换的功能。使用 Office Communicator 2007，可以从 IM 会话无缝转换到电话呼叫，然后再添加视频，所有操作都在熟悉的 Communicator “对话”窗口中进行。

用户还可以邀请其他联系人加入 IM 会话或电话呼叫，来创建 IM 会议或电话会议呼叫。

Communicator 呼叫。Office Communicator 2007 不再将联系人的 SIP URI（通常是联系人的电子邮件地址）显示为呼叫选项菜单中的菜单项，取而代之的是“Communicator 呼叫”选项。选择“Communicator 呼叫”时，它将呼叫所有运行 Office Communicator 2007 的联系人设备。根据联系人所配置的设备的不同，该呼叫可能会被拨出到联系人的计算机，也可能拨出到为 Office Communicator 2007 配置的计算机或 USB 电话设备。

23.4.2 部署 OCS 2007 客户端

1. 安装 OCS 2007 客户端

用户可以从 Microsoft 的网站下载 Office Communication 2007，其下载地址为“<http://download.microsoft.com/download/5/6/4/5642a756-3264-4da5-bb3f-5a1764414d21/CommunicatorEval.msi>”，安装过程如下。

① 运行 Office Communication 2007 的安装程序，显示如图 23-84 所示“欢迎使用 Microsoft Office Communication 2007”对话框。

② 单击“下一步”按钮，显示如图 23-85 所示的“最终用户许可协议”对话框，选择“我接受许可协议中的条款”单选按钮。

③ 单击“下一步”按钮，显示如图 23-86 所示的“配置 Microsoft Office Communicator 2007”对话框，单击“浏览”按钮，选择安装文件夹路径。



图 23-84 客户端安装向导



图 23-85 最终用户许可协议

④ 单击“下一步”按钮，Microsoft Office Communicator 007 安装程序将注册组件并完成安装，显示如图 23-87 所示的“Microsoft Office Communicator 2007 安装成功”对话框。



图 23-86 配置 Office Communicator 2007



图 23-87 Office Communicator 2007 安装成功

⑤ 单击“完成”按钮，关闭安装向导。

2. 配置客户端登录

配置 DNS 记录之后，默认情况下将 Communicator 配置为自动连接。如果需要，可以修改此设置。在每个客户端上执行以下步骤，使用户能够连接到 Office Communications Server。

① 在客户端计算机（以 Windows XP 系统为例）上，使用已准备好 OCS 客户端功能的用户账户登录到域，依次选择“开始”→“程序”→“Microsoft Office Communicator 2007”选项，打开 Microsoft Office Communicator 2007 程序，如图 23-88 所示。



图 23-88 打开选项

② 单击 Office Communicator 标题栏中的向下箭头，依次选择“工具”→“选项”选项，显示如图 23-89 所示的“选项”对话框。

③ 在“个人”选项卡上，单击“高级”按钮，显示如图 23-90 所示的“高级连接设置”对话框，选择“手动配置”单选按钮，在“内部服务器名称或 IP 地址”文本框中，输入 OCS 2007 服务器名称或 IP 地址，选择“TCP”单选按钮。

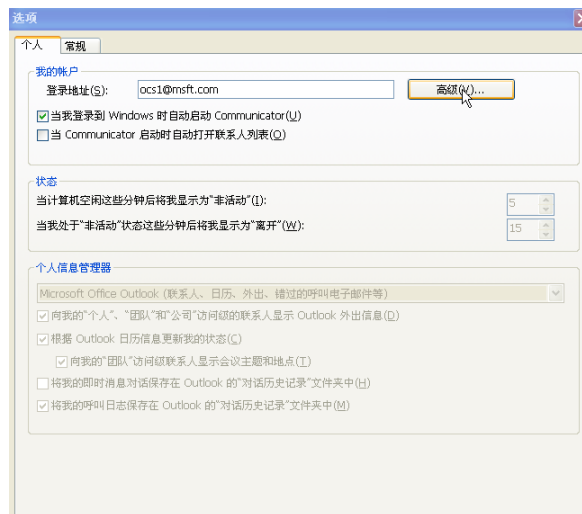


图 23-89 选项

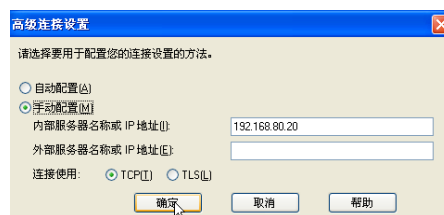


图 23-90 高级连接设置

④ 单击“确定”按钮保存设置。

完成上述配置后，返回 Office Communicator 2007 登录界面，单击“登录”按钮，即可尝试连接到 OCS 服务器，登录成功后，显示如图 23-91 所示窗口。

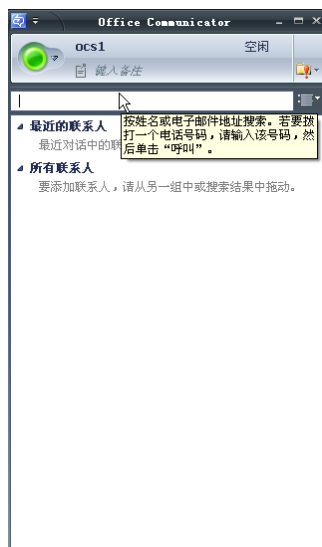


图 23-91 登录成功

3. 测试客户端配置

① 以 RTCUniversalServerAdmins 组成员的用户账户，从 B 服务器登录到域中。将 Microsoft Office Communications Server 2007 安装光盘放入光驱，部署向导将自动启动，直接单击“部署 Standard Edition Server”选项，显示如图 23-92 所示的“部署 Standard Edition Server”对话框。

② 单击“验证服务器功能”选项，显示如图 23-93 所示的“验证池或服务器功能”对话框。



图 23-92 部署 Standard Edition Server

③ 在“步骤 1：验证前端服务器设置”选项区域中，单击“运行”按钮，显示如图 23-94 所示的“欢迎使用‘Office Communications Server 2007 验证向导’”对话框。



图 23-93 验证池或服务器功能



图 23-94 OCS 2007 验证向导

④ 单击“下一步”按钮，显示如图 23-95 所示的“验证步骤”对话框，如果需要验证启用的用户是否能够登录，则选中“验证 SIP 登录（一方）和 IM（双方）”复选框。如果已将 Office Communicator 客户端配置为自动登录，并且已配置所需的 DNS 记录，则选中“选中此框可使用客户端自动登录来进行验证”复选框，以验证自动客户端登录是否起作用。

⑤ 单击“下一步”按钮，显示如图 23-96 所示的“用户帐户”对话框，输入测试用户或启用了 SIP 的用户的用户名、登录名和密码。在“服务器或池”下拉列表中，选择承载该用户的服务器。

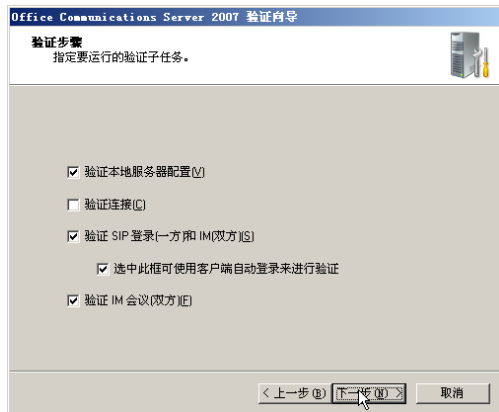


图 23-95 验证步骤

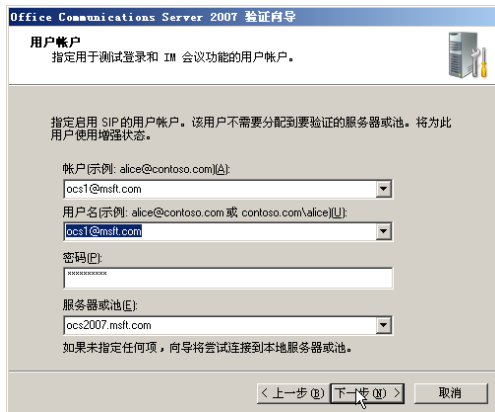


图 23-96 用户帐户

⑥ 单击“下一步”按钮，显示如图 23-97 所示“第二个用户帐户（必需）”对话框，输入另一个测试用户（为 SIP 启用的另一个用户）的用户名、登录名和密码，在“服务器或池”中，选择承载该用户的服务器。此账户将与指定的第一个账户，共同用于测试两个用户之间的 IM 功能。

⑦ 单击“下一步”按钮，显示如图 23-98 所示“联盟和公共 IM 连接”对话框，如果已经配置了联盟或公共 IM 连接，则选中“测试内部和联盟用户的连接”复选框，键入要为其测试此功能的联盟用户帐户的 SIP URI。否则，请清除此复选框。

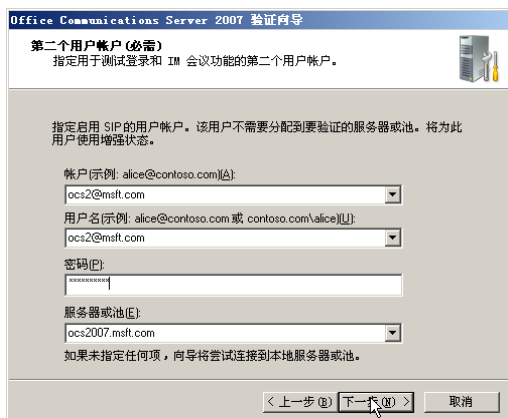


图 23-97 第二个用户帐户（必需）



图 23-98 联盟和公共 IM 连接

⑧ 单击“下一步”按钮，开始处理验证任务。完成后，显示如图 23-99 所示的“‘验证向导’已完成，但出现了警告”对话框，选中“单击‘完成’时查看日志文件”复选框。

⑨ 单击“完成”按钮，直接打开日志文件，验证“执行结果”列下是否显示为“成功”，确认服务器已成功添加到 Standard Edition Server，如图 23-100 所示。

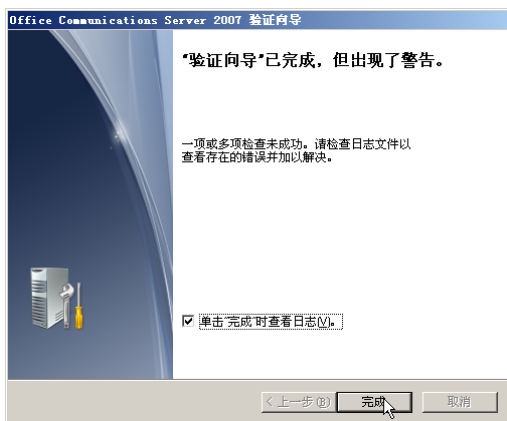


图 23-99 完成验证向导”



图 23-100 查看安装日志

4. 登录和测试 Communicator

为了验证 Communications 客户端之间的连接和通信，需要在两台不同的客户端上，使用两个已经启用 OCS 功能的用户账户登录到域。

① 在客户端计算机上，打开“Microsoft Office Communicator 2007”主程序，在“登录地址”文本框中，输入 SIP 账户名称和密码。单击“登录”按钮，登录到 OCS 服务器。在另一台客户端上执行相同的操作。如图 23-101 和图 23-102 所示为成功登录的 OCS1 和 OCS2 用户。

提示

如果提示输入凭据，则选择建议使用的格式之一即可。

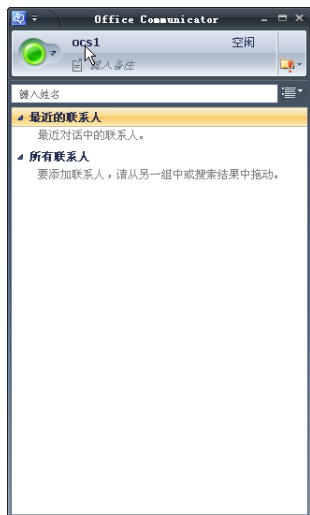


图 23-101 登录 ocs1

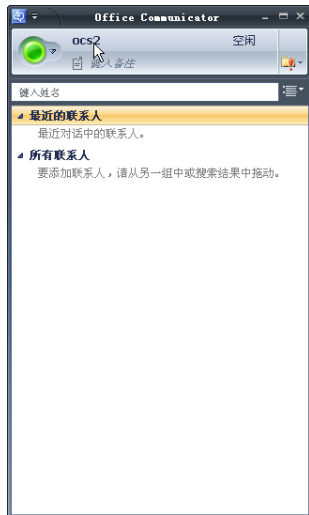


图 23-102 登录 ocs2

② 在第一台计算机上，打开 Communicator 并键入登录第二台计算机的账户的完整 SIP URI，如图 23-103 所示。

③ 在结果列表中，双击登录第二台计算机的用户的用户名，显示如图 23-104 所示的消息窗口，输入想要发送的消息，按 Enter 键即可发送。

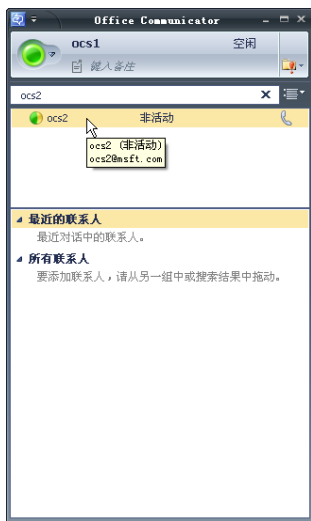


图 23-103 选择用户

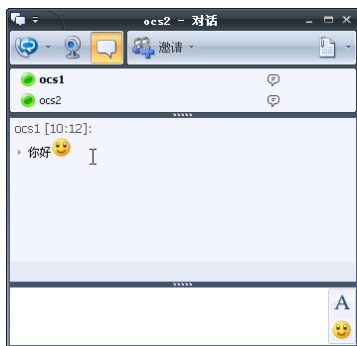


图 23-104 消息窗口

④ 在第二台计算机上，验证是否接收到消息，如图 23-105 所示。继续向对方发送一条消息，确认是否可以收到，如图 23-106 所示。



图 23-105 接受成功



图 23-106 验证成功

23.4.3 OCS 的应用

如果安装配置 Office Communication 2007 的客户端计算机, 加入到了 OCS 所属的 Active Directory 中, 使用 Active Directory 中的用户名登录到网络中, 并且在配置 Office Communication 2007 时使用当前登录的用户名所属的 SIP 账户登录, 则 Office Communication 2007 会自动登录。另外用户也可以根据需要, 对自己的 Office Communication 客户端进行相应配置。

1. 登录 OCS 客户端

① 如果更改用户登录地址, 则可以先将当前用户注销, 然后单击 Office Communicator 标题栏中的向下箭头, 依次选择“连接”→“更改登录地址”选项, 显示如图 23-107 所示的“选项”对话框, 在“个人”选项卡中的“登录地址”文本框中, 输入新的登录地址即可。

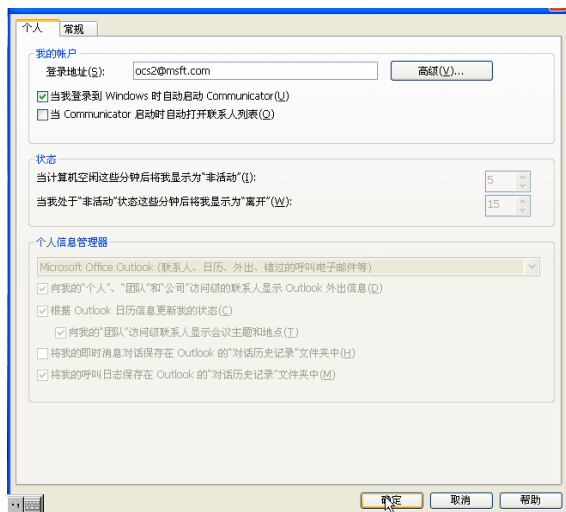


图 23-107 更改登录地址

② 单击“确定”按钮, 返回到登录界面, 如图 23-108 所示, 接下来即可使用新的地址登录到 OCS 服务器。

③ 单击“登录”按钮, 显示如图 23-109 所示的登录窗口, 分别输入“登录地址”、“用户名”和“密码”, 单击“登录”按钮, 即可以登录到 OCS 服务器。



图 23-108 登录户名



图 23-109 登录 OCS 服务器

2. OCS 客户端的使用

Office Communicator 2007 的使用很简单, 和 MSN Messenger 非常类似。可以添加联系人进行即

时消息会话，并邀请其他联系人加入会话，以及在会话中无缝添加音频和视频。

开始即时消息会话的常用方式是，双击联系人列表中的联系人姓名，显示如图 23-110 所示的“对话”窗口，在此窗口中可以输入即时消息和查看来自其他人的响应。

在即时消息中，还添加图释。图释是可以用来在即时消息中表达心情和情绪的图形图像，如图 23-111 所示。

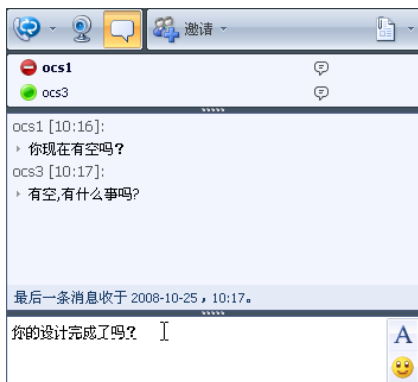


图 23-110 对话窗口



图 23-111 使用图释

23.5 Live Meeting 2007 的部署与应用

Live Meeting 2007 可以为用户提供计划会议、演示会议以及共享演示文稿等实用功能。另外，新版本的 Live Meeting 还增加了以下新功能：

音频和视频选项。Microsoft Office Live Meeting 同时增强了计算机音频和电话会议功能。用户可以使用网络摄像机显示一位或多位演示者的视频。在使用计算机音频的会议中，视频将主动切换到当前演讲者。用户还可以使用 Microsoft RoundTable 通信和存档系统向远程参与者显示会议室的全景视频，也可以通过连接两个会议室在位于不同地点的两个工作组之间举行会议。

讲义。作为演示者，用户可以在会议之前或会议期间分发与会者可以下载的内容。

共享说明。用户可以创建并保存所有与会者都能够看到的说明。

参加会议。收到 Microsoft Office Live Meeting 的电子邮件邀请时，可以通过单击邀请中的链接轻松加入会议。该电子邮件邀请还包含有关在计算机上安装会议客户端的信息。正式连接到会议时，可以通过多种方式查看会议并进行参与。

23.5.1 部署 Live Meeting 2007

Live Meeting 2007 客户端的安装非常简单，用户可以在安装向导的帮助下顺利完成。安装完成后，可以按照如下步骤进行相关配置。

① 依次单击“开始”→“所有程序”→“Microsoft Office Live Meeting 2007”→“Microsoft Office Live Meeting 2007”选项，打开 Live Meeting 2007 客户端主程序。

② 单击标题栏的向下箭头，选择下拉菜单中的“打开用户帐户”选项，显示如图 23-112 所示的“测试连接”对话框。

③ 在“登录名”文本框中输入客户端登录地址，如 ocs1@msft.com，单击“测试连接”按钮，验证是否可以登录到 OCS 服务器，如果测试成功，则显示如图 23-113 所示的“测试成功”对话框。



图 23-112 测试连接



图 23-113 测试成功

如果当前登录用户已被授予组织会议权限，则在“欢迎使用 Microsoft Office Live Meeting”窗口中，将显示“立即开会”按钮，如图 23-114 所示。单击“立即开会”按钮，在 Live Meeting 客户端中，单击“会议”菜单，检查是否显示为“已连接”状态，如图 23-115 所示。如果成功建立连接，则可以开始会议。



图 23-114 欢迎使用 Microsoft Office Live Meeting

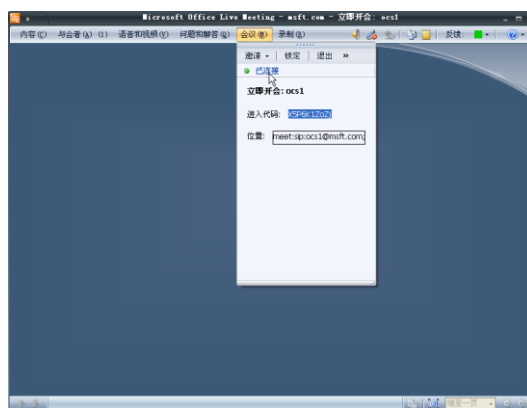


图 23-115 查看连接成功

23.5.2 Live Meeting 2007 客户端的应用

Office Live Meeting 客户端窗口的菜单栏，包括了丰富的应用功能。根据会议的设置方式以及是否具有使用某些功能的权限，菜单项目也会有所不同。在会议期间，演示者可以显示准备好的演示文稿，也可以在 Office Live Meeting 客户端中创建新的演示文稿页面。用户可以导入 Office PowerPoint 演示文稿图形程序文档（.ppt）或 Live Meeting 文档（.lmp 或 .pwp），也可以上载到 Office Document Image (MODI) Writer 的文档，其中包括 Office Word（.doc、.docx）和 Office Excel（.xls、.xlsx）文档。

1. 向与会者显示演示文稿或文档

在 Office Live Meeting 客户端窗口中，依次单击“内容”→“共享”→“上载文件（仅视图）”选项，显示“打开”对话框，导航到要添加的文件，单击“打开”按钮，显示“上载文件（仅视图）”对话框。单击“继续”按钮，Office Live Meeting 会将文件转换为 Live Meeting 格式，并将其添加到“内容”列表中，如图 23-116 所示。

2. 创建白板

在 Office Live Meeting 客户端窗口中，依次单击“内容”→“共享”→“白板”选项，显示如图 23-117 所示“白板”窗口，单击位于窗口底部的绘图和文本工具，即可在“白板”中创建内容，该内容将同时显示在其他与会者的窗口中。

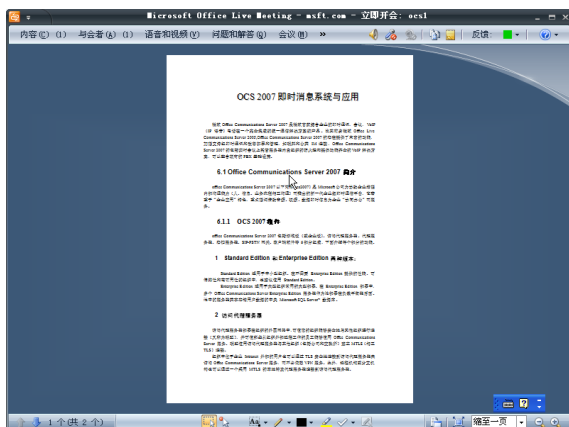


图 23-116 向与会者显示演示文稿或文档

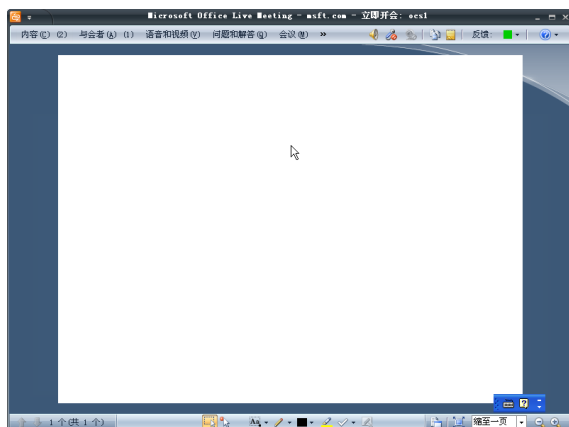


图 23-117 白板

3. 创建文本页

在 Office Live Meeting 客户端窗口中, 依次单击“内容”→“共享”→“文本页”选项, 显示如图 23-118 所示“文本页”窗口, 单击位于窗口底部的绘图和文本工具即可创建内容。

4. 共享网页

在 Office Live Meeting 客户端窗口中, 依次单击“内容”→“共享”→“网页”选项, 显示“新建网页”对话框, 键入要将与与会者指向的网页 URL, 如: www.baidu.com。单击“验证网页”按钮, 显示“网页检查”对话框。如果网页显示正确, 则单击“创建网页”按钮, 即可共享该网页, 如图 23-119 所示。

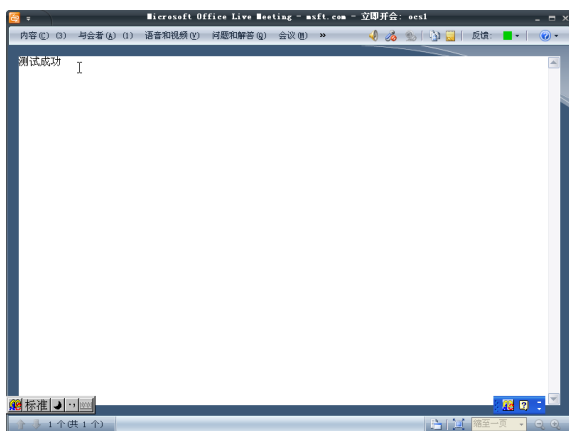


图 23-118 文本页



图 23-119 共享网页

5. 录制会议

通过录制会议功能, 可以录制会议的数据、音频和视频部分, 作为存档。

(1) 在 Office Live Meeting 客户端窗口中, 单击“录制”→“选项”选项, 显示如图 23-120 所示“个人录制选项”对话框, 选择要录制的所有会议选项(包括“数据”、“语音”、“视频”和“全景视频”)。如果要更改已录制的会议的保存位置, 则可以单击“更改”按钮, 导航到要保存录制的文件夹。

(2) 单击“录制”按钮, 即可开始录制。需要停止时, 单击“停止”按钮, 选择“录制”菜单中的“保存录制”选项, 即可保存录制内容。

录制完成后, 依次单击“开始”→“所有程序”→“Microsoft Office Live Meeting 2007”→“Microsoft Office Live Meeting 录制管理器”, 即可查看录制的内容, 如图 23-121 所示。

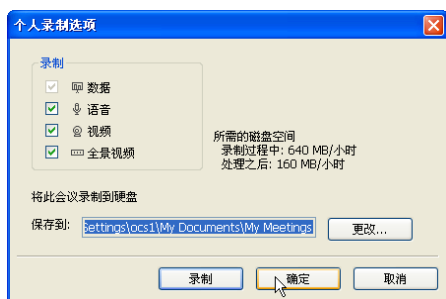


图 23-120 个人录制选项

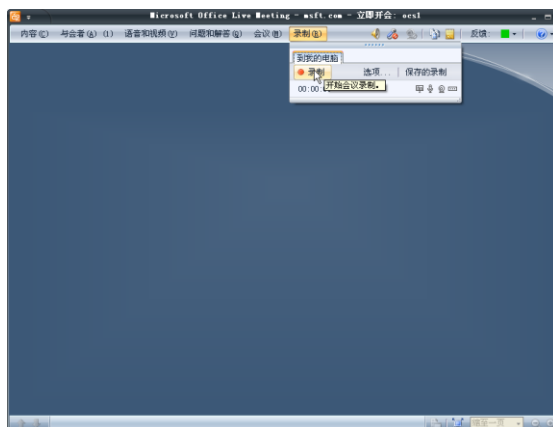


图 23-121 检查录制

23.6 Outlook 会议外接程序

如果在域中配置了邮件服务器，使用 Outlook 会议的外接程序，可以更充分地利用 Live Meeting 2007 的功能，使用 Office Communicator 2007，可以轻松地从一个 IM 会话中开始会议。另外，还可以将各种通信模式添加到会议会话中，包括电话、视频设备，甚至是使用 Live Meeting 的全 Web 会议和数据共享。

23.6.1 配置 Outlook 的会议外接程序

Outlook 客户端是 Microsoft Office System 中的组件之一，安装过程比较简单，此处不做详细介绍。客户端计算机上安装 Microsoft Outlook 2003 及以上版本后，即可开始配置 Outlook 的会议外接程序。

- ① 依次单击“开始”→“程序”→“Microsoft Office”→“Microsoft Office Outlook 2003”选项，启动 Outlook 2003。
- ② 单击“下一步”按钮，显示如图 23-122 所示的“电子邮件账户”对话框，选择“是”单选按钮。
- ③ 单击“下一步”按钮，显示如图 23-123 所示的“服务器类型”对话框，选择“Microsoft Exchange Server”单选按钮。

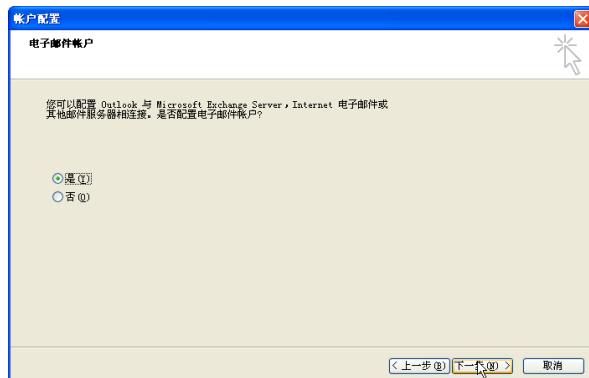


图 23-122 电子邮件账户

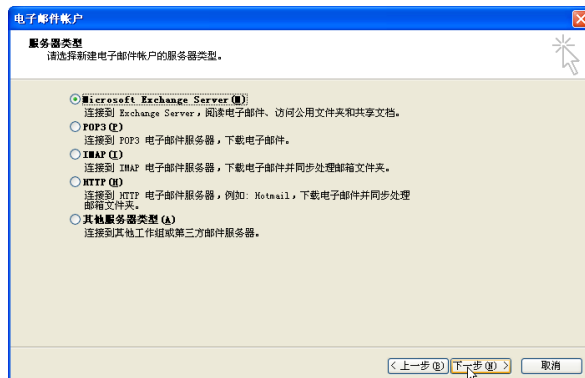


图 23-123 服务器类型

- ④ 单击“下一步”按钮，显示如图 23-124 所示的“Exchange Server 设置”对话框，设置 Exchange Server 的 IP 地址，输入用户名，单击“检查姓名”按钮，确认到服务器的连通性。
- ⑤ 单击“下一步”按钮，显示如图 23-125 所示的“祝贺您”对话框，电子邮件设置完成。

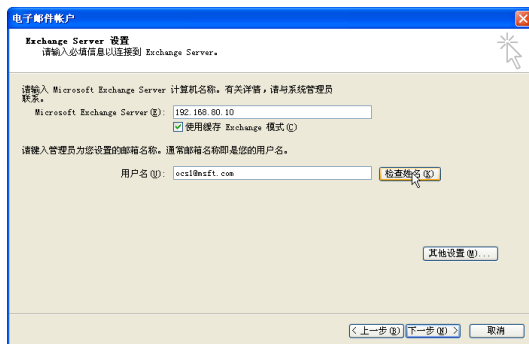


图 23-124 Exchange Server 设置



图 23-125 祝贺您

23.6.2 创建会议并加入会议

1. 计划会议

① 依次单击“开始”→“所有程序”→“Microsoft Office”→“Microsoft Office Outlook 2003”选项，显示如图 23-126 所示的 Outlook 主窗口。

② 单击“计划 Live Meeting”按钮，显示如图 23-127 所示的窗口。在“约会”选项卡中的“主题”文本框中，键入会议的相关说明，在“收件人”文本框中，输入被邀请者的电子邮件地址。

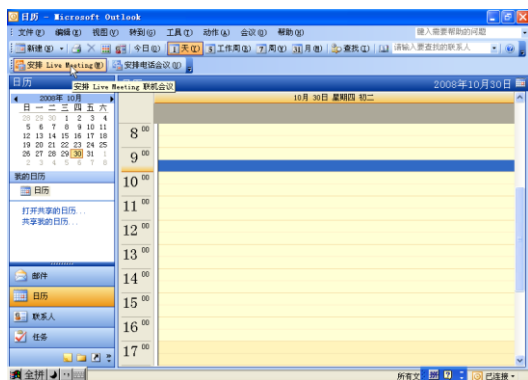


图 23-126 Outlook 主窗口

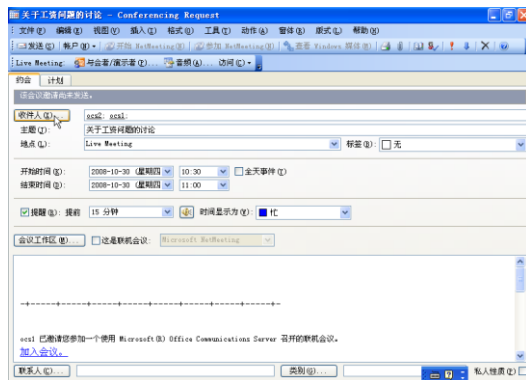


图 23-127 计划 Live Meeting

③ 单击“收件人”按钮，显示如图 23-128 的“选择与会者及资源”对话框，选择所添加的收件人，然后单击“确定”按钮，将其添加到“收件人”文本框中。

④ 单击“与会者/演示者”按钮，显示如图 23-129 所示的“与会者和演示者”对话框，在“与会者”列表中选择用户名，单击“添加”按钮，将其添加到“演示者”列表中。单击“确定”按钮，保存设置。



图 23-128 选择与会者及资源

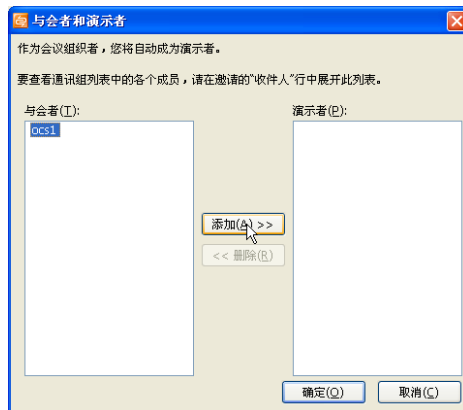


图 23-129 与会者和演示者

⑤ 单击“音频”按钮，显示如图 23-130 所示的“Live Meeting 音频选项”对话框。如果要使参与者能够使用耳麦或麦克风和扬声器的计算机进行连接，则选择“使用计算机音频连接到会议”单选按钮，单击“确定”按钮，保存设置。

⑥ 单击“发送”按钮，开始向所选用户发送会议邀请，如图 23-131 所示。

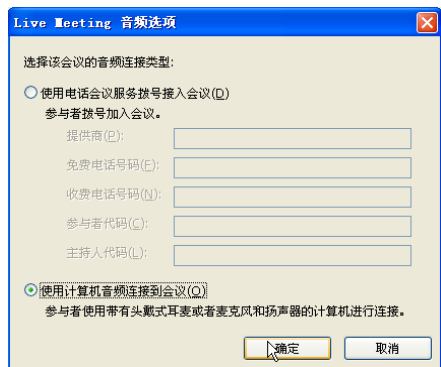


图 23-130 选择音频

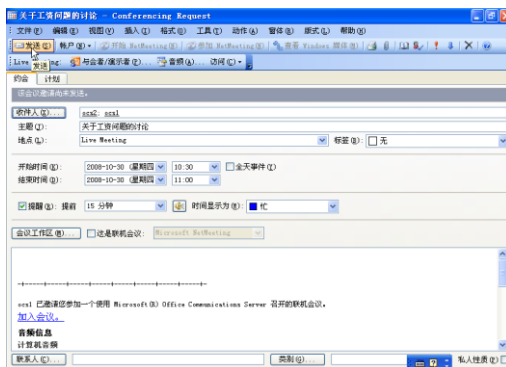


图 23-131 发送

⑦ 发送过程中会显示“提醒”对话框，单击“清除”按钮即可。收件人 ocs2 在收件箱中打开邮件，单击“加入会议”链接，即可尝试接受邀请，参加会议，如图 23-132 所示。

⑧ 成功加入会议后，显示如图 23-133 所示窗口，Live Meeting 会显示用户当前状态：在会议中。

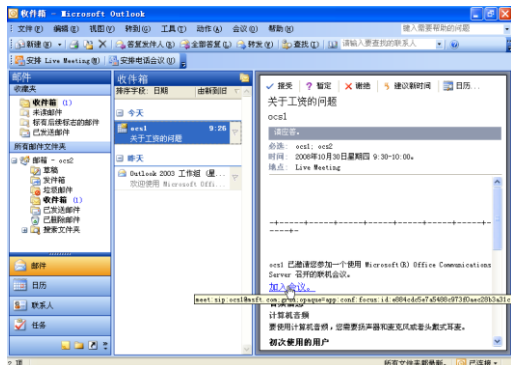


图 23-132 ocs2 加入会议

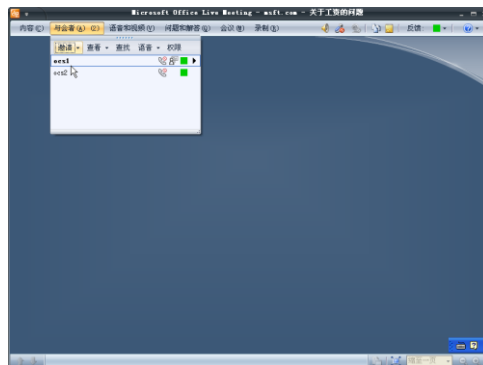


图 23-133 加入成功

2. 发起会议

① 在 Office Communicator 2007 客户端窗口中，右击想要邀请的联系人（以 ocs2 为例），选择快捷菜单中的“安排会议”选项，显示如图 23-134 所示的“会议”窗口。输入“主题”、“地点”和“标签”等信息。

② 单击“发送”按钮，发送邀请邮件。收件人在收到的电子邮件中，单击“加入会议”链接即可参加会议，如图 23-135 所示。

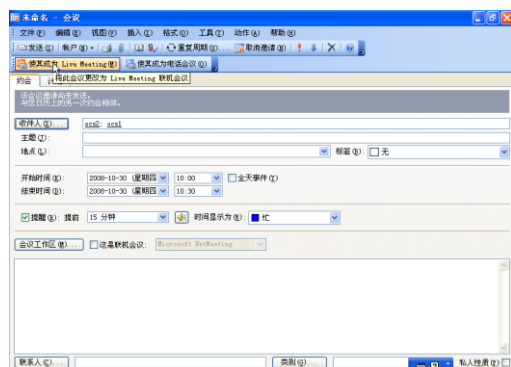


图 23-134 会议

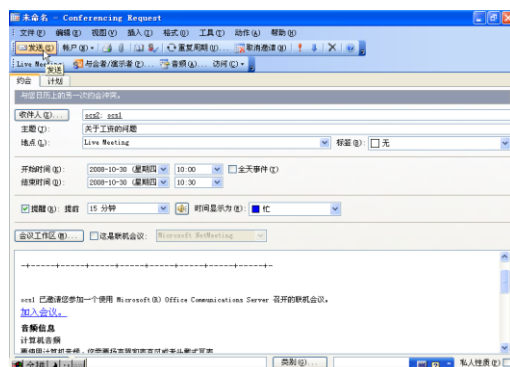


图 23-135 邀请邮件

3. 开始临时的“立即开会”会议

通过使用“立即开会”选项，可以随时开始会议，而不用提前进行计划，开始会议后，即可邀请其他与会者。

① 依次单击“开始”→“所有程序”→“Microsoft Office Live Meeting 2007”→“Microsoft Office Live Meeting 2007”选项，显示如图 23-136 所示的“欢迎使用 Microsoft Office Live Meeting”窗口。



图 23-136 立即开会

② 单击“立即开会”按钮，打开如图 23-137 所示“立即开会”窗口。

③ 依次单击“与会者”→“邀请”→“通过电子邮件”选项，显示如图 23-138 所示“立即开会 ocs1 邮件”窗口，在“收件人”文本框中，输入想要邀请的用户，如果同时指定多个收件人，则可以用分号将每个地址隔开。

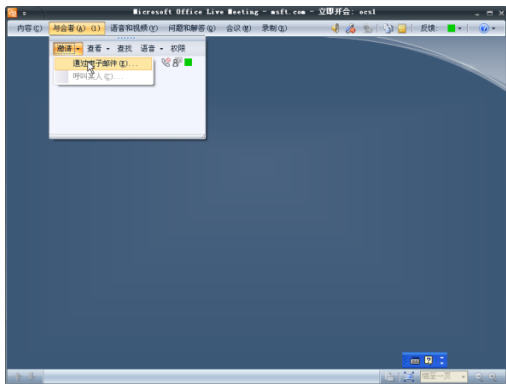


图 23-137 邀请与会者

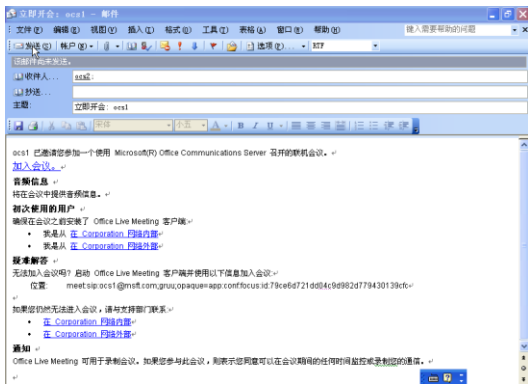


图 23-138 发送电子邮件

④ 单击“发送”按钮，即可发送邀请邮件。收件人打开邮件后，显示如图 23-139 所示窗口。

⑤ 单击“加入会议”链接，即可加入会议，如图 23-140 所示。

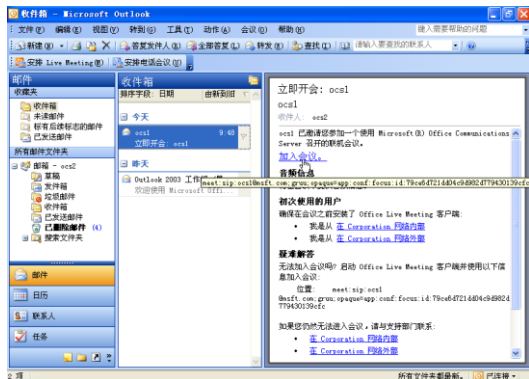


图 23-139 收到邀请邮件

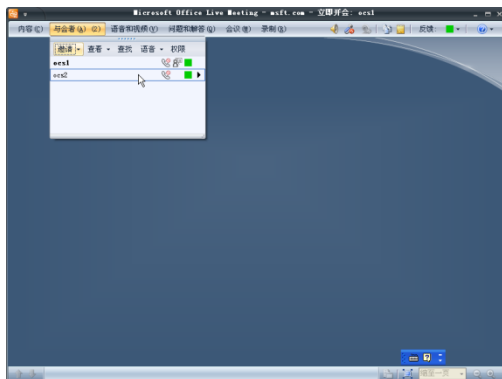


图 23-140 成功加入会议

第 24 章 Hyper-V

Windows Server 2008 x64 操作系统支持服务器虚拟化功能，称为 Hyper-V，即“服务器虚拟技术”。Hyper-V 服务器虚拟化和 Virtual server 2005 R2 不同，Virtual server 2005 R2 是安装在物理计算机操作系统之上的一个应用程序，被物理计算机运行的操作系统管理。运行 Hyper-V 的物理计算机使用的操作系统和虚拟机使用的操作系统，运行在底层的 Hypervisor 之上，物理计算机使用的操作系统实际上相当于一个特殊的虚拟机操作系统，和真正的虚拟机操作系统平级，因此 Hyper-V 创建的虚拟机不能算成传统意义上的虚拟机，可以认为是一台独立的计算机。

24.1 Hyper-V 概述

Hyper-V 可以让多个操作系统共享一个硬件，而各个操作系统就好像一台独立的计算机。Hyper-V 直接接管虚拟机管理工作，把系统资源划分为多个分区。其中主操作系统所在的分区叫做父分区，虚拟机所在的分区叫做子分区，可以确保虚拟机的性能最大化，几乎可以接近物理机器的性能，性能高于 Virtual PC/Virtual Server 基于模拟器创建的虚拟机。

►► 24.1.1 Hyper-V 系统需求

安装 Windows Server 2008 Hyper-V 功能硬件基本需要如下：

CPU：最少 1GHz，建议 2GHz 以及速度更快的 CPU。

内存：最少 512 MB，建议 1GB 以上。

- 完整安装 Windows Server 2008 建议 2GB 内存。
- 安装 64 位标准版，最多支持 32GB 内存。
- 安装 64 位企业版或者数据中心版，最多支持 2TB 内存。

磁盘：完整安装 Windows Server 2008 建议 40GB 磁盘空间；安装 Server Core 建议 10GB 磁盘空间。如果硬件条件许可，建议将 Windows Server 2008 安装在 Raid5 磁盘阵列或者具备冗余功能的磁盘设备中。

其他基本硬件，DVD-ROM、键盘、鼠标、Super VGA 显示器等。

Hyper-V 对硬件的要求比较高，主要集中在 CPU 方面：

- (1) CPU 必须支持硬件虚拟化功能，例如 Intel VT 技术或者 AMD-V 技术。
- (2) CPU 必须支持 X64 位技术。
- (3) CPU 必须支持硬件 DEP (Date Execution Prevention 数据执行保护) 技术，即 CPU 防病毒技术。
- (4) 系统的 BIOS 设置必须开启硬件虚拟化等设置，默认关闭 CPU 的硬件虚拟化功能。
- (5) Windows Server 2008 必须使用 x64 版本，x86 版本不支持虚拟化功能。

目前，主流服务器 CPU 均支持以上要求，只要支持硬件虚拟化功能，其他两个要求基本都能够满足。为了安全起见，在购置硬件设备之前，最好事先到 CPU 厂商的网站上确认 CPU 的型号是否满足以上要求。

►► 24.1.2 Hyper-V 优点

相对 Virtual PC/Virtual Server 创建的虚拟机，Hyper-V 创建的虚拟机除了高性能之外，Hyper-V 虚拟机至少还具有以下优点：

多核支持，可以为每个虚拟机分配 8 个逻辑处理器，利用多处理器核心的并行处理优势，对要求大量计算的大型工作负载进行虚拟化，物理主机要具有多内核。而 Virtual PC/Server 只能使用一个内核。

支持创建 x64 位的虚拟机，Virtual PC/Server 如果要创建 x64 的虚拟机，宿主操作系统必须使用 x64 操作系统，然后安装 X64 的 Virtual PC/Server 应用系统。

使用卷影副本（Shadow Copy）功能，Hyper-V 可以实现任意数量的 SnapShot（快照）。可以创建“父-子-子”模式以及“父-并列子”模式的虚拟机，而几乎不影响虚拟机的性能。

支持内存的“写时复制”（Copy on Write）功能，多个虚拟机如果采用相同的操作系统，可以共享同一个内存页面，如果某个虚拟机需要修改该共享页面，可以在写入时复制该页面。

支持非 Windows 操作系统，例如 Linux 操作系统。

支持 WMI 管理模式，可以通过 WSH 或者 PowerShell 对 Hyper-V 进行管理，也可以通过 MMC 管理单元对 Hyper-V 进行管理。

Hyper-V 支持 Server Core 操作系统，可以将 Windows Server 2008 的服务器核心安装用作主机操作系统。服务器核心具有最低安装需求和低开销，可以提供尽可能多的主服务器处理能力来运行虚拟机。

在 System Center Virtual Machine Manager 2007 R2 等产品的支持下，Hyper-V 支持 P2V（物理机到虚拟机）的迁移，可以把虚拟机从一台计算机无缝迁移到另外一台计算机上（虚拟机无需停机），支持根据虚拟机 CPU、内存或者网络资源的利用率设置触发事件，自动给运行关键业务的虚拟机热添加 CPU、内存或者网络资源等功能。

Hyper-V 创建的虚拟机（X86）支持 32GB 的内存，Virtual Server 虚拟机最多支持 16.6GB 内存。

Hyper-V 虚拟机支持 64 位 Guest OS，最大内存支持 64GB。

高性能，在 Hyper-V 中，物理机器上的 Windows OS 和虚拟机的 Guest OS，都运行在底层的 Hyper-V 之上，所以物理操作系统实际上相当于一个特殊的虚拟机操作系统，只是拥有一些特殊权限。

Hyper-V 采用完全不同的系统架构，性能接近于物理机器，这是 Virtual Server 无法比拟的。

提供远程桌面连接功能。

支持动态添加硬件功能，Hyper-V 可以在受支持的来宾操作系统运行时向其动态添加逻辑处理器、内存、网络适配器和存储器。此功能便于对来宾操作系统精确分配 Hyper-V 主机处理能力。

网络配置灵活，Hyper-V 为虚拟机提供高级网络功能，包括 NAT、防火墙和 VLAN 分配，这种灵活性可用于创建更好地支持网络安全要求的 Windows Server Virtualization 配置。

支持磁盘访问传递功能，可以将来宾操作系统配置为直接访问本地或 iSCSI 存储区域网络（SAN）存储，为产生大量 I/O 操作的应用程序（如 SQL Server 或 Microsoft Exchange）提供更高的性能。

提高服务器的利用率，正常应用中，一台服务器的利用率在 10% 左右。通过运行几个虚拟服务器，可以将利用率提高到在 60% 或 70%，减少硬件投资。

24.2 安装与配置 Hyper-V

Windows Server 2008 x64 操作系统安装完成后，默认并没有安装 Hyper-V 角色，需要手动通过“添加角色向导”进行安装。安装完成后，需要配置 Hyper-V 服务器和虚拟机。

►► 24.2.1 安装 Hyper-V 角色

Hyper-V 的安装十分简单，通过“添加角色向导”即可完成角色的安装。不同的版本 Hyper-V 角色安装不尽相同，请参考 Windows Server 2008 操作系统帮助文件。

- ① 打开“服务器管理器”窗口，启动“添加角色向导”，当显示“选择服务器角色”对话框时，在“角色”列表中，选中“Hyper-V”复选框，用于安装 Hyper-V 服务，如图 24-1 所示。
- ② 单击“下一步”按钮，显示如图 24-2 所示的“Hyper-V”对话框，简要介绍了 Hyper-V 的功能。



图 24-1 “选择服务器角色”对话框



图 24-2 “Hyper-V”对话框

- ③ 单击“下一步”按钮，显示如图 24-3 所示的“创建虚拟网络”对话框。在“以太网卡”列表中，选择需要用于虚拟网络的物理网卡，建议至少为物理计算机保留一块物理网卡。
- ④ 单击“下一步”按钮，显示如图 24-4 所示的“确认安装选择”对话框。

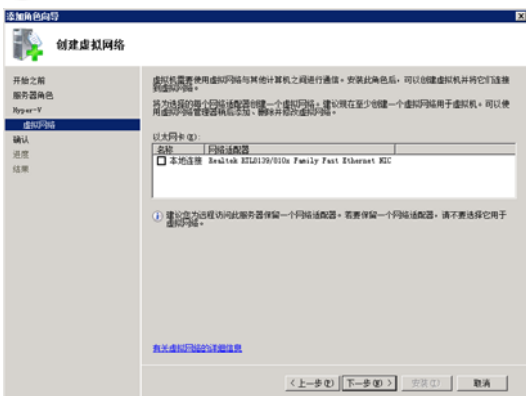


图 24-3 “创建虚拟网络”对话框



图 24-4 “确认安装选择”对话框

- ⑤ 单击“安装”按钮，开始安装 Hyper-V 角色。完成后，显示如图 24-5 所示的“安装结果”对话框，提示需要重新启动服务器完成安装。
- ⑥ 单击“关闭”按钮，显示如图 24-6 所示的“添加角色向导”对话框。单击“是”按钮，重新启动服务器。



图 24-5 “安装结果”对话框

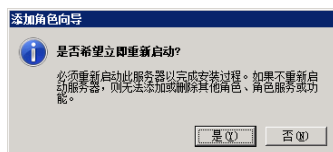


图 24-6 提示重新启动

⑦ 服务器重新启动后，继续执行安装进程。安装后显示如图 24-7 所示的“安装结果”对话框，单击“关闭”按钮，完成 Hyper-V 角色的安装。

⑧ 在“服务器管理器”窗口中，展开“角色”→“Hyper-V”→“Hyper-V Manager”，如图 24-8 所示。



图 24-7 “安装结果”对话框

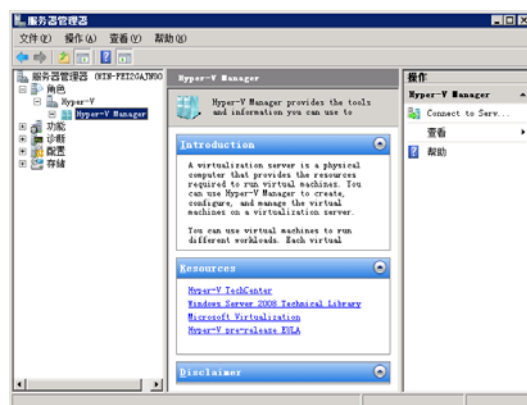


图 24-8 “服务器管理器”窗口

24.2.2 配置 Hyper-V 服务器

服务器配置，对该服务器上所有虚拟机生效，提供创建虚拟机、虚拟磁盘、虚拟网络、虚拟磁盘整理、删除服务器、停止服务以及启动服务等操作。

1. New 选项

创建新的虚拟机、虚拟磁盘以及虚拟软盘。

① 在“服务器管理器”窗口中，选择“服务器管理器”→“角色”→“Hyper-V”→“Hyper-V Manager”→服务器名称，如图 24-9 所示。

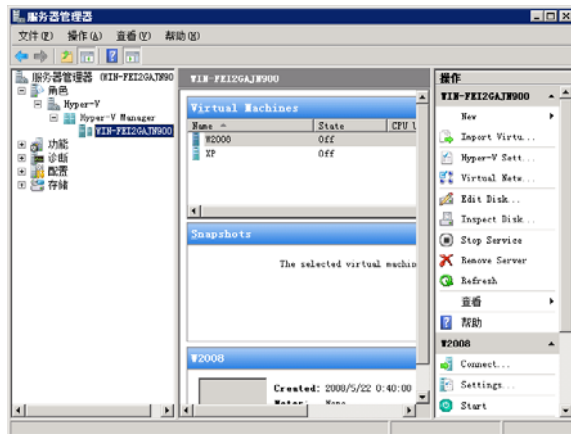


图 24-9 “服务器管理器”窗口

② 右击目标服务器，在快捷菜单中选择“New”级联菜单，选择“Virtual Machine”命令，可启动创建虚拟机向导。

③ 选择“New”→“Hard Disk”命令，启动创建虚拟磁盘向导。

④ 选择“New”→“Floppy Disk”命令，启动创建虚拟软盘向导。

2. Import Virtual Machine 选项

导入虚拟机。

① 右击目标服务器，在快捷菜单中选择“Import Virtual Machine”命令，显示如图 24-10 所示的“Import Virtual Machine”对话框。单击“Browse”按钮选择目标文件夹，或者直接键入文件夹路径，如图 24-10

所示。

- ② 单击“Import”按钮，将虚拟机导入服务器中，如图 24-11 所示。

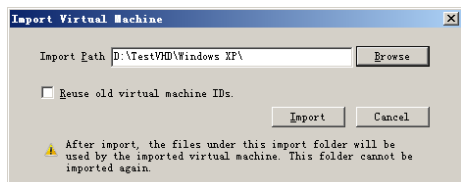


图 24-10 “Import Virtual Machine”对话框

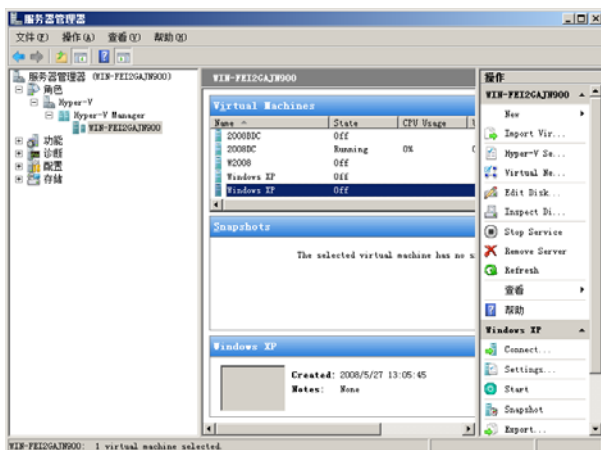


图 24-11 “服务器管理器”窗口

3. Hyper-V Settings 选项

- (1) 设置 Windows Server Virtualization 参数。

右击目标服务器，在快捷菜单中选择“Hyper-V Settings”命令，显示如图 24-12 所示的“Hyper-V Settings”对话框。

- (2) 设置 Virtual Hard Disks 参数。

设置虚拟磁盘默认存储文件夹。

- ① 选择“Server”→“Virtual Hard Disks”选项，显示如图 24-13 所示的对话框。默认存储虚拟磁盘文件夹位置为 C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks。

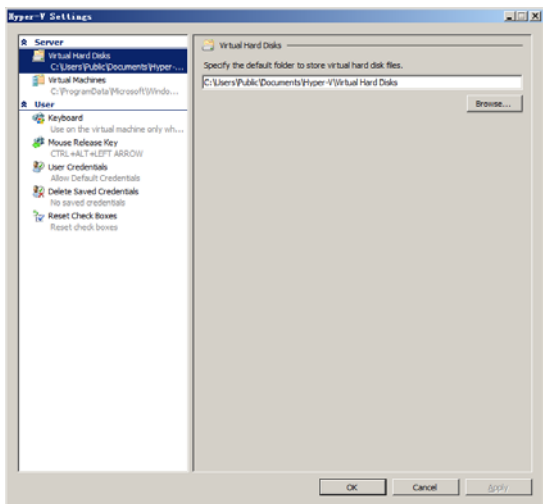


图 24-12 “Hyper-V Settings”对话框

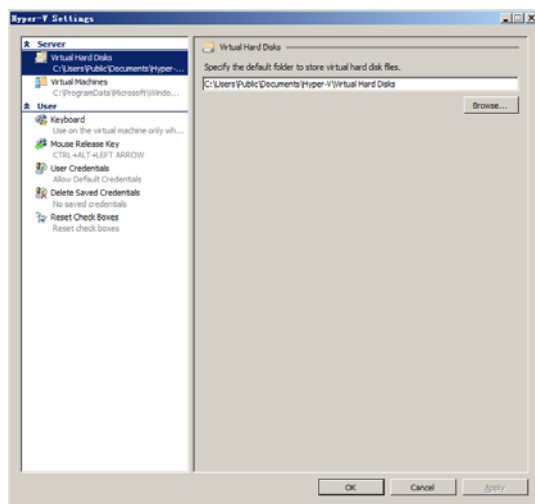


图 24-13 Virtual Hard Disks 参数

- ② 单击“Browse”按钮，选择目标文件夹。单击“OK”按钮，完成虚拟磁盘存储位置的设置。

- (3) 设置 Virtual Machines 参数

设置虚拟机默认存储文件夹。

- ① 选择“Server”→“Virtual Machines”选项，显示如图 24-14 所示的对话框。默认虚拟机配置文件存储文件夹位置为 C:\ProgramData\Microsoft\Windows\Hyper-V。单击“Browse”按钮，选择目标文件夹。

② 单击“OK”按钮，完成虚拟磁盘存储位置的设置。

(4) 设置 Keyboard 参数

设置键盘功能键。

选择“User”→“Keyboard”选项，显示如图 24-15 所示的对话框，设置键盘中的功能键生效的场合，提供 3 个选项，分别为：物理计算机中使用，虚拟机中使用，以及虚拟机全屏幕操作时使用。根据需要选择即可。

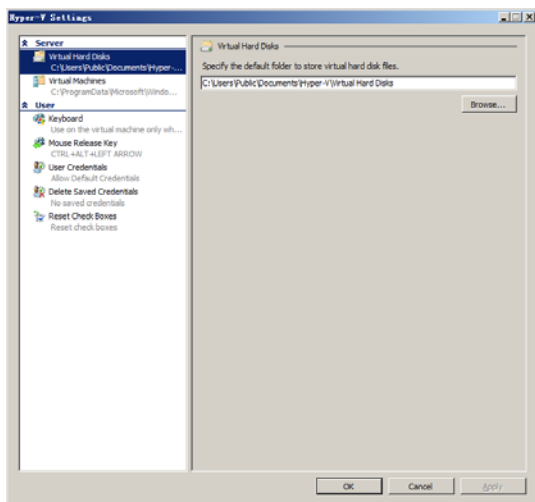


图 24-14 Virtual Machines 参数

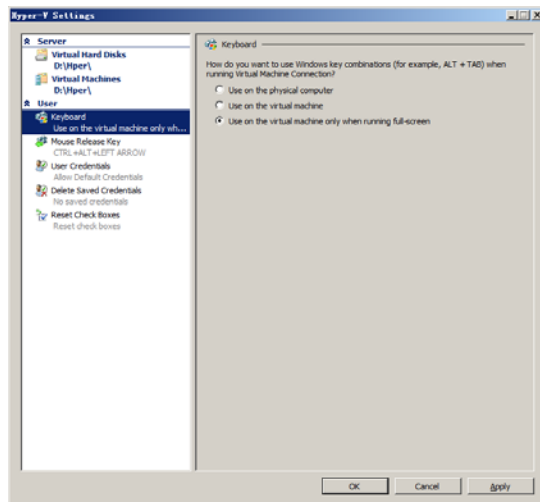


图 24-15 Keyboard 参数

(5) 设置 Mouse Release Key 参数

设置鼠标释放快捷键。

选择“User”→“Mouse Release Key”选项，显示如图 24-16 所示的对话框。设置鼠标在虚拟机中使用时，切换到物理计算机使用的快捷键，默认快捷键为“Ctrl+Alt+LEFT ARROW”，即 Ctrl+Alt+左箭头。提供 3 个选项，分别为：Ctrl+Alt+LEFT ARROW、Ctrl+Alt+RIGHT ARROW、Ctrl+Alt+Space 以及 Ctrl+Alt+Shift。根据需要选择即可。

(6) 设置 User Credentials 参数

设置用户证书。

选择“User”→“User Credentials”选项，显示如图 24-17 所示的对话框。在物理计算机和虚拟机之间连接时，使用默认用户证书进行验证。

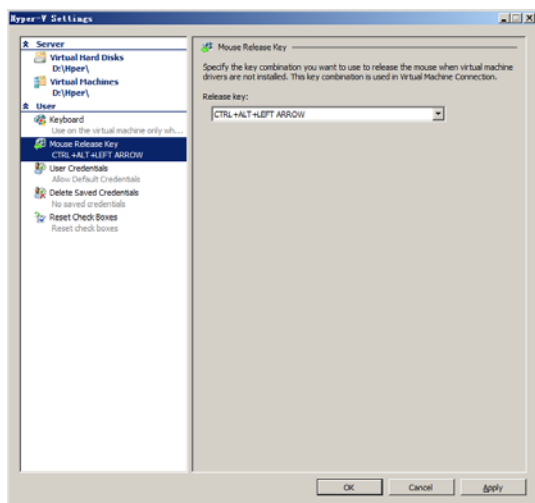


图 24-16 Mouse Release Key 参数

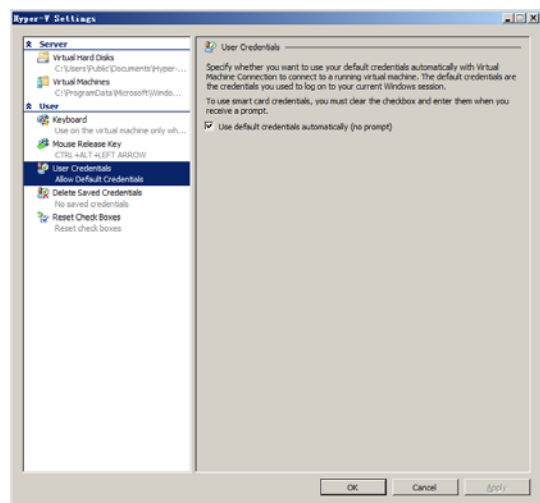


图 24-17 User Credentials 参数

(7) 设置 Delete Saved Credentials 参数

删除已经安装的用户证书。

选择“User”→“Delete Saved Credentials”选项，显示如图 24-18 所示的对话框。单击“Delete”按钮，删除安装在物理计算机中的用户证书。如果当前计算机中没有安装证书，则“Delete”按钮不可用。

(8) 设置 Reset Check Boxes 参数

重置复选框。

选择“User”→“Reset Check Boxes”选项，显示如图 24-19 所示的对话框。单击“Reset”按钮，恢复原始设置。

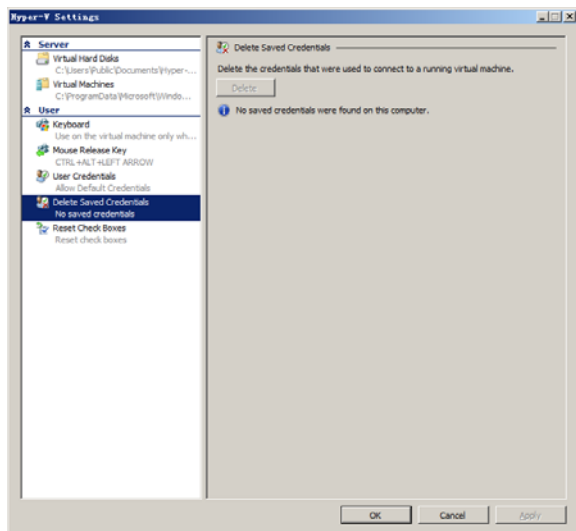


图 24-18 Delete Saved Credentials 参数

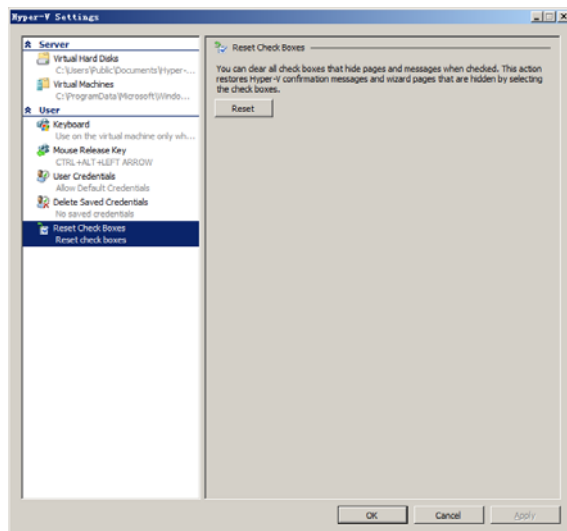


图 24-19 Reset Check Boxes 参数

4. Virtual Network Management 选项

设置虚拟网络。

右击目标服务器，在快捷菜单中选择“Virtual Network Management”命令，显示如图 24-20 所示的“Virtual Network Management”对话框，设置虚拟环境使用的网络参数。

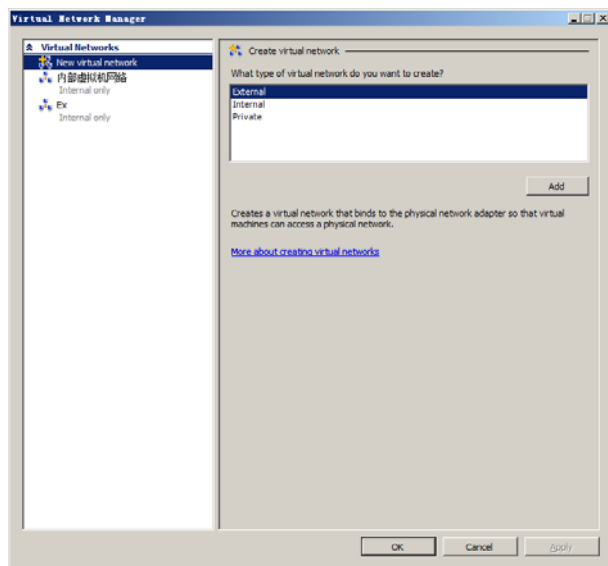


图 24-20 “Virtual Network Management”对话框

5. Edit Disk 选项

压缩、合并以及扩容虚拟磁盘。

右击目标服务器，在快捷菜单中选择“Edit Disk”命令，启动虚拟磁盘整理向导，显示如图 24-21 所示的“Before You Begin”对话框，向导根据虚拟磁盘的设置整合不同的功能。

6. Inspect Disk 选项

检查虚拟磁盘，检查选择的虚拟磁盘的类型，如果是差异虚拟磁盘，则逐级检查关联的虚拟磁盘。

① 右击目标服务器，在快捷菜单中选择“Inspect Disk”命令，显示如图 24-22 所示的“打开”对话框，选择需要检查的虚拟磁盘。

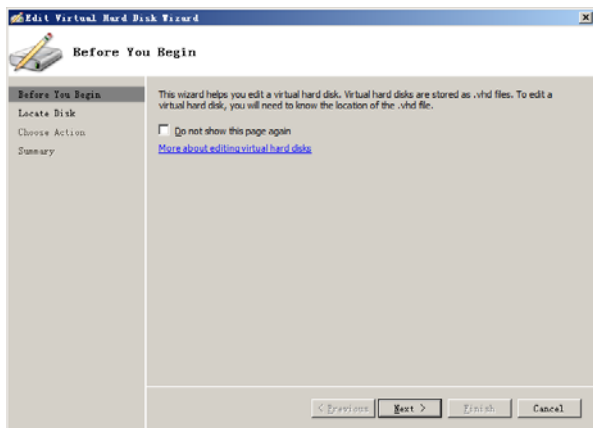


图 24-21 “Before You Begin”对话框

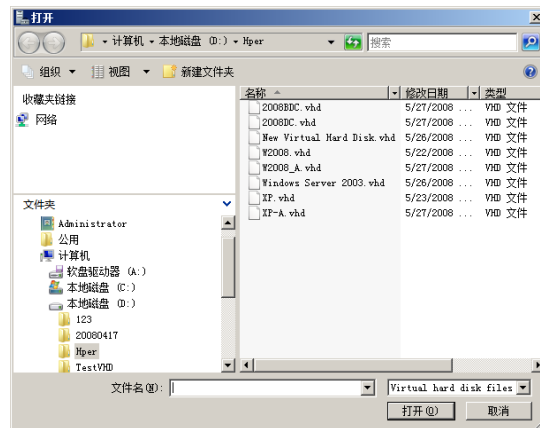


图 24-22 “打开”对话框

② 选择好虚拟磁盘后，单击“打开”按钮，显示如图 24-23 所示的“Virtual Hard Disk Properties”对话框，显示选择的虚拟磁盘的参数。

③ 单击“Close”按钮，完成虚拟磁盘的检查。

7. Remove Server 选项

删除目标服务器。

右击目标服务器，在快捷菜单中选择“Remove Server”命令，直接删除选择的服务器，服务器删除后，将返回到上级菜单，如图 24-24 所示。

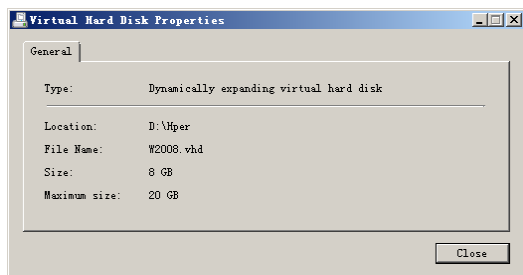


图 24-23 Virtual Hard Disk Properties

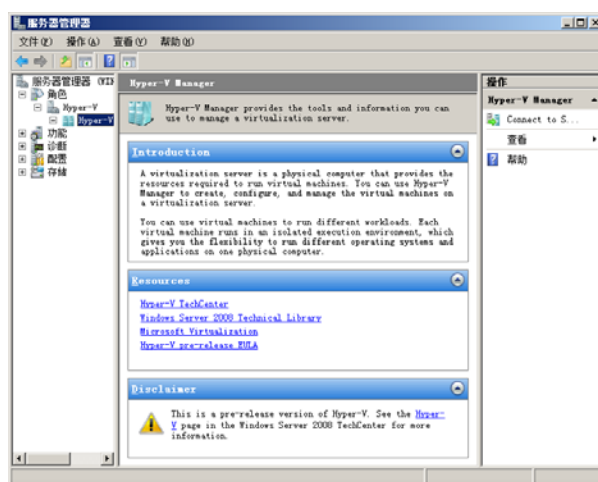


图 24-24 Remove Server 选项

8. Stop Service 选项

停止虚拟机管理服务。

① 右击目标服务器，在快捷菜单中选择“Stop Service”命令，显示如图 24-25 所示的“Stop Virtual Machine Management service”对话框。

② 单击“是”按钮，停止虚拟机管理服务，在管理窗口中将不显示该物理计算机中安装的任何虚拟机，如图 24-26 所示。

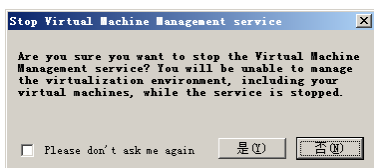


图 24-25 Stop Virtual Machine Management service

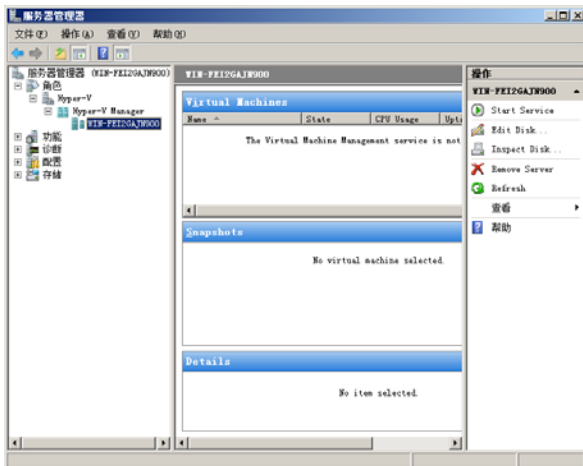


图 24-26 停止虚拟机管理服务

9. Start Service 选项

启动虚拟机管理服务。

右击目标服务器，在快捷菜单中选择“Start Service”命令，启动虚拟机管理服务，如图 24-27 所示。

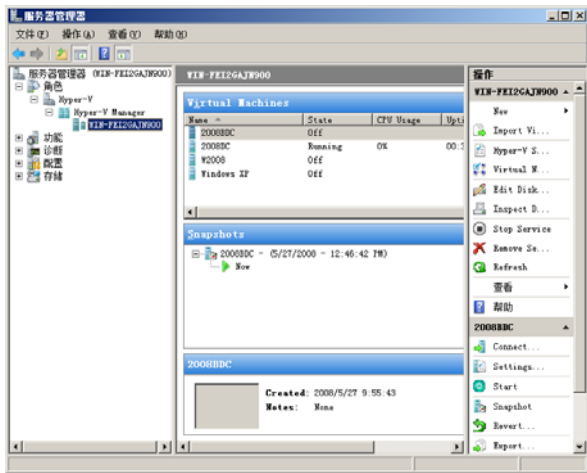


图 24-27 Start Service 选项

24.2.3 配置虚拟机

虚拟机配置，仅对选择的虚拟机生效，包括虚拟机启动、暂停、关机、虚拟机的关联设备、快照、重命名以及删除虚拟机等，该配置对虚拟机管理器同样有效。

在“服务器管理器”窗口的“Virtual Machines”面板中，选择目标虚拟机。右击目标虚拟机，显示如图 24-28 所示的功能菜单，显示基于虚拟机功能菜单。

1. Connect 选项

连接到虚拟机。

右击目标虚拟机，在快捷菜单中选择“Connect”命令，启动虚拟机管理器，显示如图 24-29 所示的窗口，在窗口中显示当前虚拟机的状态。

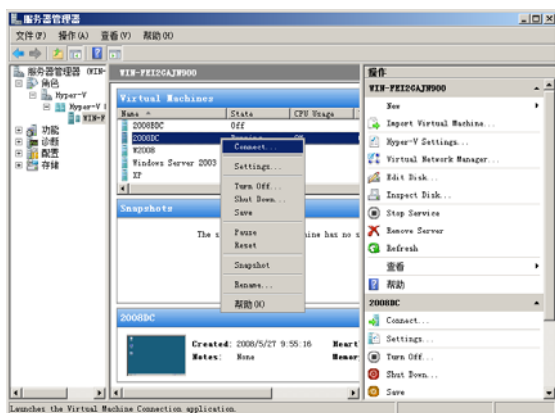


图 24-28 “服务器管理器”窗口

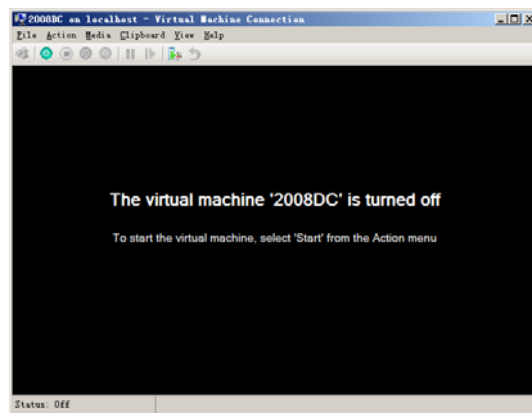


图 24-29 Connect 选项

2. Settings 选项

配置虚拟机参数。

右击目标虚拟机，在快捷菜单中选择“Settings”命令，显示如图 24-30 所示的对话框。

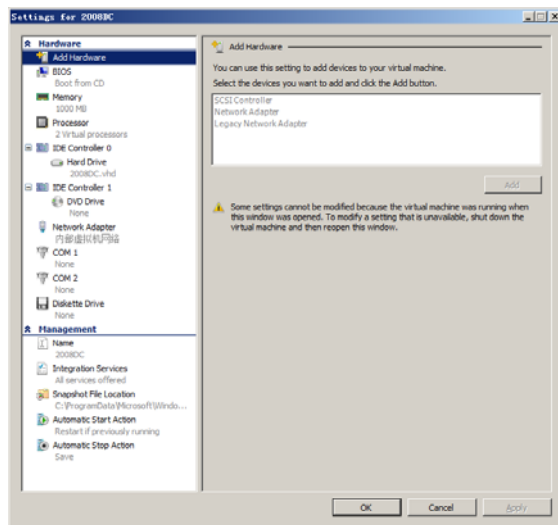


图 24-30 Settings 选项

3. TurnOff 选项

关闭虚拟机电源。

右击目标虚拟机，在快捷菜单中选择“Turn Off”命令，显示如图 24-31 所示的“Turn Off Machine”对话框。

单击“Turn Off”按钮，关闭正在运行的虚拟机。

4. Shutdown 选项

关闭虚拟机。

右击目标虚拟机，在快捷菜单中选择“Shutdown”命令，显示如图 24-32 所示的“Shut Down Machine”对话框。

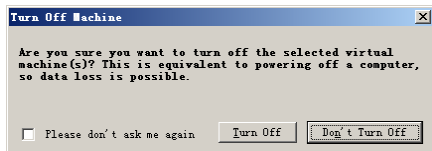


图 24-31 “Turn Off Machine”对话框

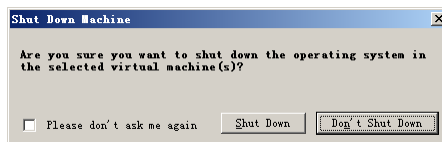


图 24-32 “Shut Down Machine”对话框

单击“Shut Down”按钮，关闭正在运行的虚拟机。

5. Save 选项

保存虚拟机的状态。

① 右击目标虚拟机，在快捷菜单中选择“Save”命令，虚拟机的状态由“Running”转变为“Saving”，如图 24-33 所示。

② 保存完成后，虚拟机的状态由“Saving”转变为“Saved”，如图 24-34 所示。

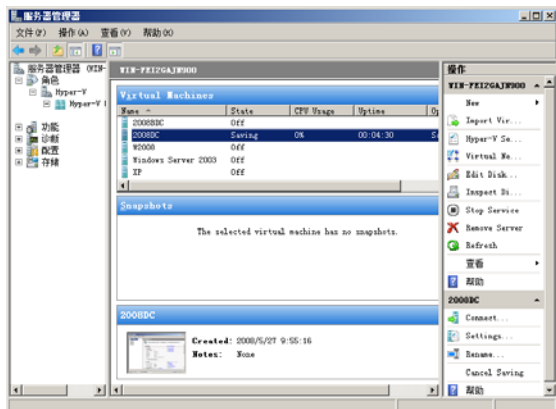


图 24-33 Save 选项

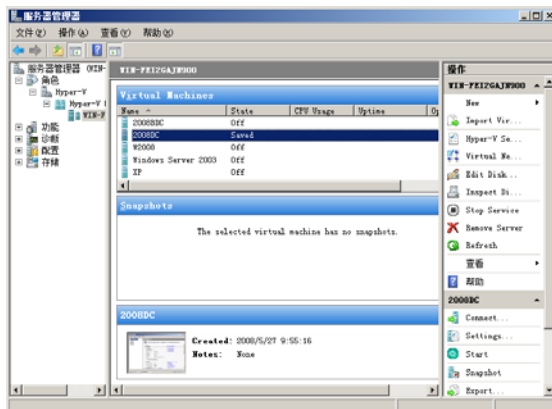


图 24-34 Save 选项

6. Start 选项

启动虚拟机。

右击目标虚拟机，在快捷菜单中选择“Start”命令，启动虚拟机，如图 24-35 所示。

7. Reset 选项

初始化虚拟机，相当于物理计算机的复位键。

① 右击目标虚拟机，在快捷菜单中选择“Reset”命令，显示如图 24-36 所示的“Test Machine”对话框。

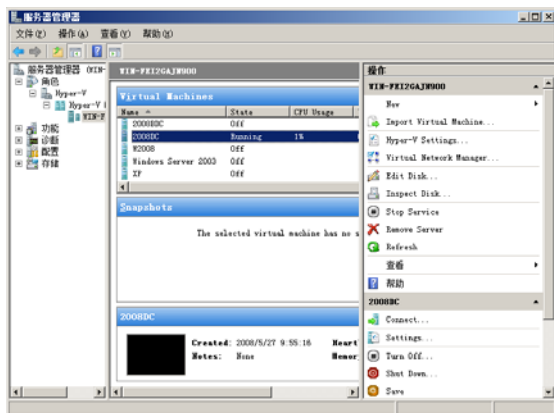


图 24-35 Start 选项

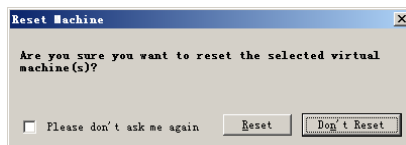


图 24-36 “Test Machine”对话框

② 单击“Reset”按钮，重新启动虚拟机。

8. Snapshot 选项

创建虚拟机快照。

右击目标虚拟机，在快捷菜单中选择“Snapshot”命令，在选择的虚拟机基础上创建快照，如图 24-37 所示。

9. Export 选项

导出虚拟机。只有在虚拟机停止的状态下，方可导出虚拟机的状态。

① 右击目标虚拟机，在快捷菜单中选择“Export”命令，显示“Export Virtual Machine”对话框。单击“Browse”按钮，选择虚拟机保存目标文件夹，如图 24-38 所示。

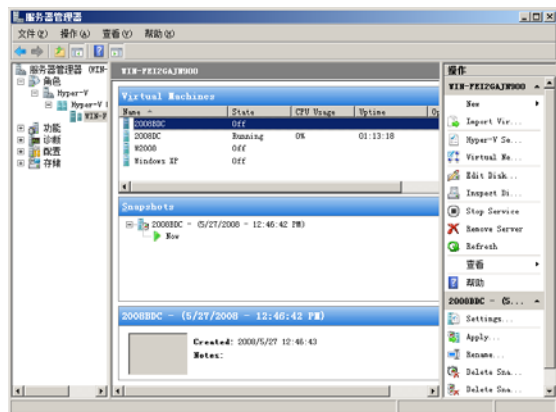


图 24-37 Snapshot 选项

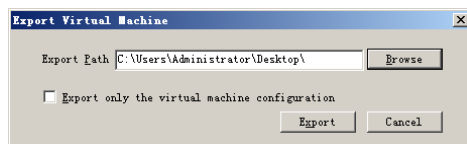


图 24-38 “Export Virtual Machine”对话框

② 单击“Export”按钮，导出虚拟机。成功导出的虚拟机包含一组文件，分别为：Virtual Machines、Virtual Hard Disks 以及 Snapshots。

10. Rename 选项

重命名虚拟机。

① 右击目标虚拟机，在快捷菜单中选择“Rename”命令，直接更改虚拟机的名称，如图 24-39 所示。

② 更改完成，按“Enter”键后保存。

11. Delete 选项

删除虚拟机。

① 右击目标虚拟机，在快捷菜单中选择“Delete”命令，显示如图 24-40 所示的“Delete Virtual Machine”对话框。

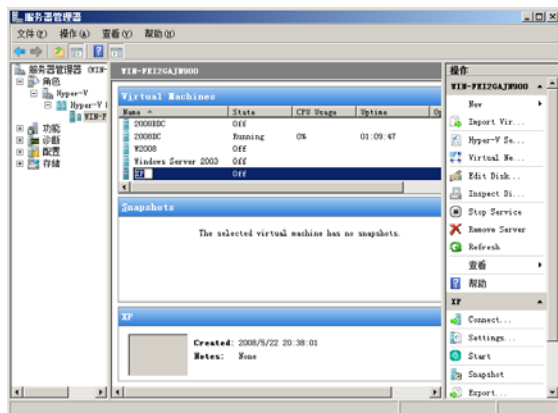


图 24-39 Rename 选项

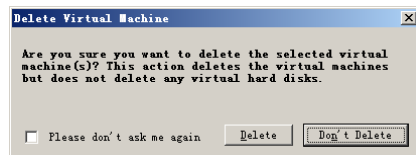


图 24-40 “Delete Virtual Machine”对话框

② 单击“Delete”按钮，删除目标虚拟机。

12. Pause 选项

暂停虚拟机的运行。

右击目标虚拟机，在快捷菜单中选择“Pause”命令，暂停虚拟机运行，如图 24-41 所示，虚拟机的状态由“Running”转变为“Paused”。

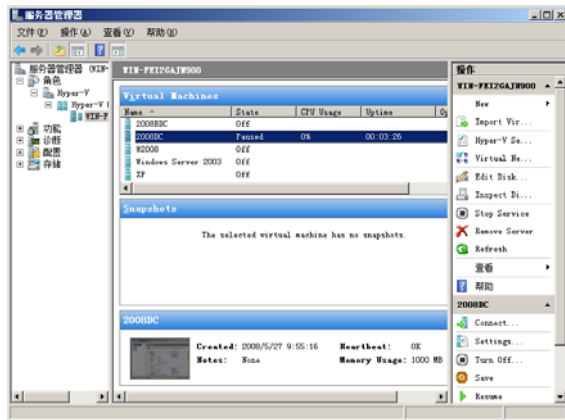


图 24-41 Pause 选项

13. Resume 选项

继续运行虚拟机。

右击已经停止运行的虚拟机，在快捷菜单中选择“Resume”命令，继续运行虚拟机，如图 24-42 所示，虚拟机的状态由“Paused”转变为“Running”。



图 24-42 Resume 选项

24.3 创建虚拟网络

Hyper-V 支持“虚拟网络”功能，提供多种网络模式，设置的虚拟网络将影响宿主操作系统的网络设置。对 Hyper-V 进行初始配置时需要为虚拟环境提供一块用于通信的物理网卡，当完成配置后，会为当前的宿主操作系统添加一块虚拟网卡，用于宿主操作系统与网络的通信。而此时的物理网卡除了作为网络的物理连接外，还兼做虚拟交换机，为宿主操作系统及虚拟机操作系统提供网络通信。

Hyper-V 提供 3 种网络虚拟交换机功能，分别为：

Hyper-V Internal Network，此类交换机只能连接到 Hyper-V 创建的虚拟机中，换句话说只能在虚拟机之间通信。

Hyper-V External Network，连接到宿主计算机上的某一块网卡。在 Hyper-V 上配置外部网络后，自动添加一块虚拟网卡用于宿主操作系统通信，而物理网卡则用于物理连接及虚拟交换机，

如图 24-43 所示。

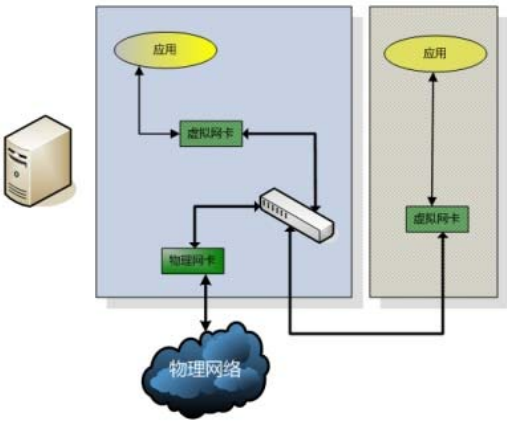


图 24-43 Hyper-V External Network 通信模式

Hyper-V Private Network，私有网络。

创建虚拟网络的操作步骤如下：

- ① 在“服务器管理器”窗口右侧的“操作”面板中，单击“Virtual Network Manager”超链接，打开虚拟网络配置对话框，显示如图 24-44 所示的“Virtual Network Manager”对话框。
- ② 单击“Add”按钮，显示如图 24-45 所示的“Virtual Network Manager”对话框。

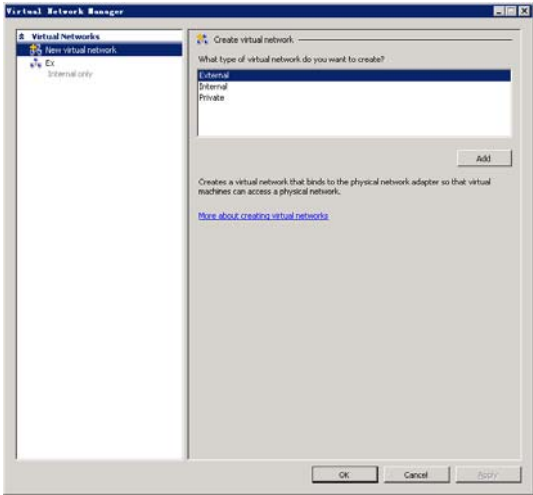


图 24-44 “Virtual Network Manager”对话框

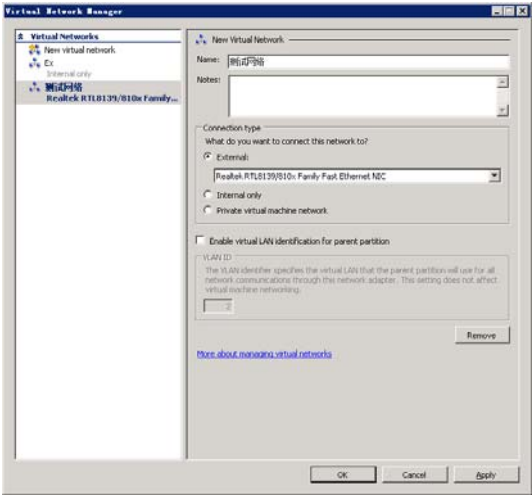


图 24-45 “Virtual Network Manager”对话框

在“Name”文本框中，键入虚拟网络的名称。

在“Connection type”文本框中，选择虚拟网络类型。如果选择“External”和“Internal”类型，将可以设置虚拟网络所在的“Vlan”区域。如果选择“Private virtual machine network”类型，不提供“Vlan”设置功能。本例中选择“Internal”类型的虚拟网络，在网卡下拉列表中选择关联的网卡。

选择“Enabled virtual LAN identification for parent partition”选项，设置新创建的虚拟网络所处的 VLAN，如图 24-46 所示。

单击“OK”按钮，完成虚拟网络设置。

- ③ 选择“开始”→“控制面板”→“网络和共享中心”选项，打开“网络和共享中心”窗口。单击“管理网络连接”超链接，选择用于虚拟机之间连接的网络连接，右击并在快捷菜单中选择“状态”命令，显示如图 24-47 所示的“本地连接状态”对话框，显示当前连接的速度为 10GB。

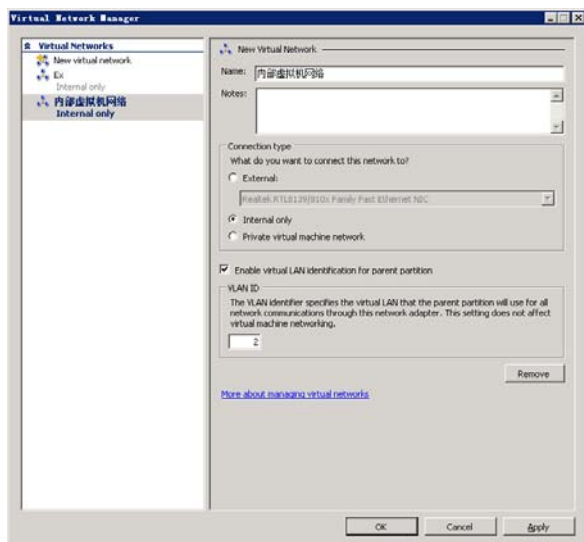


图 24-46 “Virtual Network Manager” 对话框

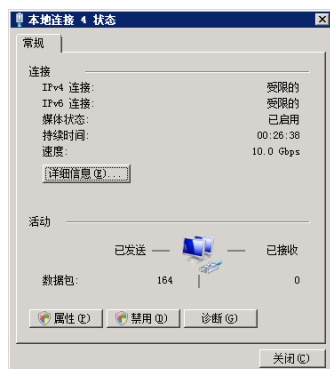


图 24-47 “本地连接 4 状态” 对话框

24.4 创建虚拟磁盘

虚拟磁盘存储虚拟机运行的主体，包括运行的操作系统及应用程序，虚拟磁盘可以在服务器之间复制，如果创建的虚拟磁盘类型为差异虚拟磁盘，在服务器之间复制时，需要将父虚拟磁盘和子虚拟磁盘一起复制，建议父子存放在同一个目录下。

24.4.1 创建虚拟磁盘

虚拟磁盘可以单独创建，也可以在创建虚拟机时创建，如果要使用差异虚拟磁盘，则建议使用“虚拟磁盘创建向导”完成虚拟磁盘的创建。

① 打开“服务器管理器”窗口，右击服务器名，选择“New”→“Hard Disk”命令，启动“New Virtual Hard Disk”向导，创建新的虚拟磁盘。

② 单击“Next”按钮，显示如图 24-48 所示的“Choose Disk Type”对话框，选择虚拟磁盘的类型，Hyper-V 支持“动态扩展硬盘”、“固定大小硬盘”以及“差异虚拟磁盘”3 中类型，本例选择“动态扩展硬盘”，即“Dynamically expanding”选项。

③ 单击“Next”按钮，显示如图 24-49 所示的“Specify Name and Location”对话框，设置虚拟磁盘名称以及存储的目标文件夹。单击“Browse”按钮选择目标文件夹。

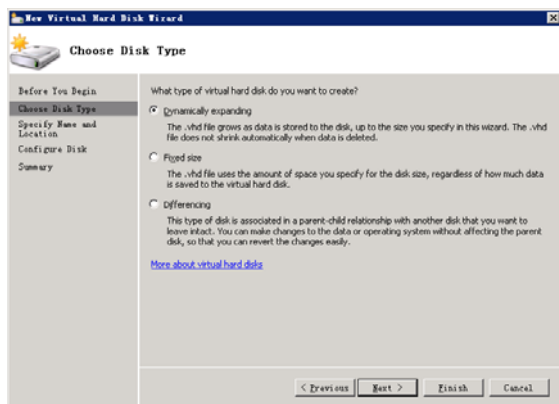


图 24-48 Choose Disk Type

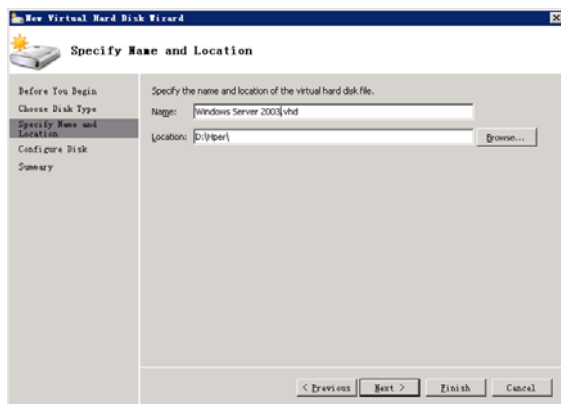


图 24-49 Specify Name and Location

④ 单击“Next”按钮，显示如图 24-50 所示的“Configure Disk”对话框，配置虚拟磁盘参数。在“Size”文本框中，键入创建的虚拟磁盘大小。

⑤ 单击“Next”按钮，显示如图 24-51 所示的“Completing the New Virtual Hard Disk Wizard”对话框，显示虚拟磁盘的配置信息。

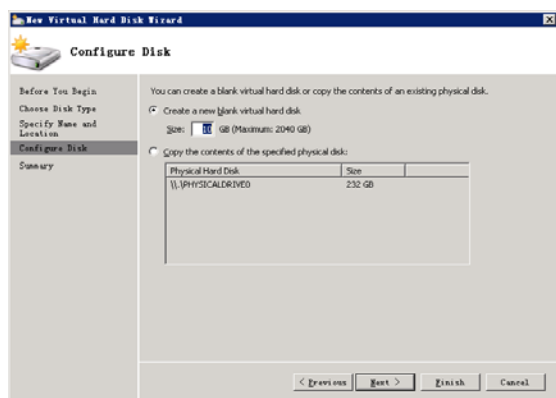


图 24-50 配置虚拟磁盘参数

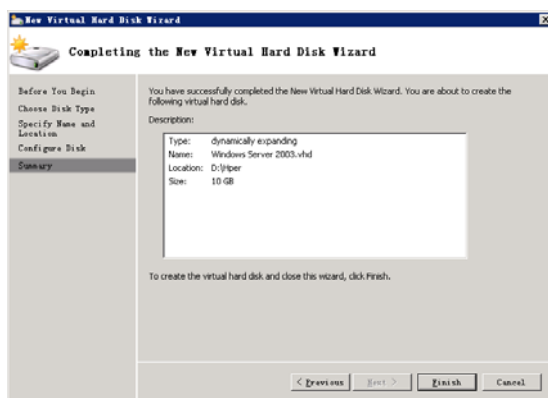


图 24-51 虚拟磁盘的配置信息

⑥ 单击“Finish”按钮，完成虚拟磁盘的创建。

24.4.2 配置虚拟磁盘

虚拟磁盘配置完成后，或者使用一段时间之后，硬盘的占用空间将变大，此时可以使用硬盘压缩功能，整理磁盘空间。使用差异虚拟磁盘时，也可以将子硬盘合并到父虚拟磁盘中。

① 在“服务器管理器”窗口，单击“Edit Disk”超链接，启动磁盘整理向导。

② 单击“Next”按钮，显示“Locate Virtual Hard Disk”对话框，单击“Browse”按钮，选择需要目标虚拟磁盘，如图 24-52 所示。

③ 单击“Next”按钮，显示如图 24-53 所示的“Choose Action”对话框，选择需要完成的功能。该向导提供 3 种磁盘处理功能：压缩磁盘、磁盘转换以及磁盘扩展功能。

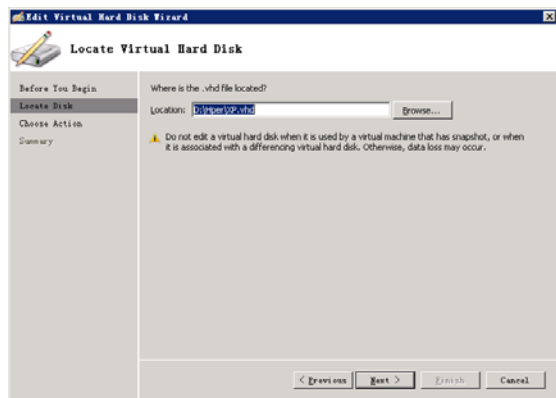


图 24-52 选择虚拟磁盘

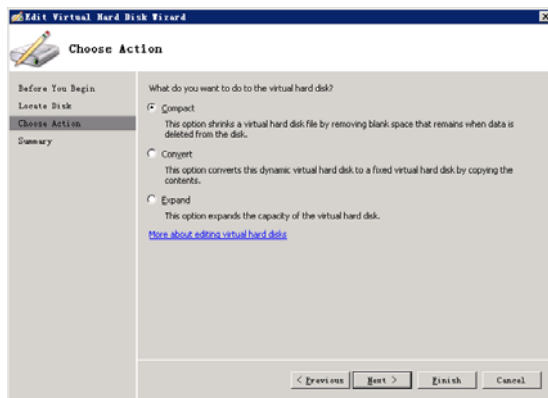


图 24-53 选择功能

④ 在“Choose Action”对话框中，选择“Compact”选项，启动磁盘“压缩磁盘”功能，单击“Next”按钮，显示如图 24-54 所示的“Completing the Edit Virtual Hard Disk Wizard”对话框。单击“Finish”按钮，处理完成自动关闭该对话框

⑤ 在“Choose Action”对话框中，选择“Convert”选项，将选择的磁盘转换为固定大小的磁盘。单击“Next”按钮，显示如图 24-55 所示的“Convert Virtual Hard Disk”对话框。在“Name”文本框中，键入转换后的虚拟磁盘的名称。单击“Finish”按钮。

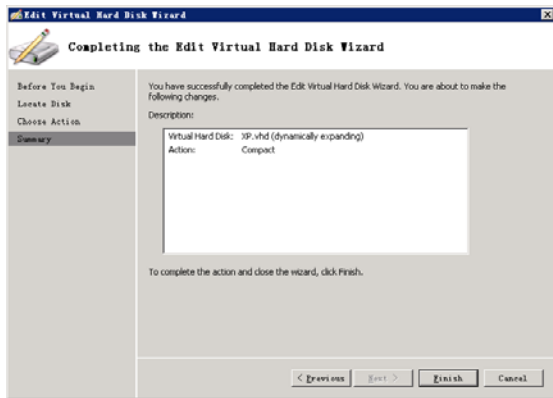


图 24-54 压缩磁盘功能

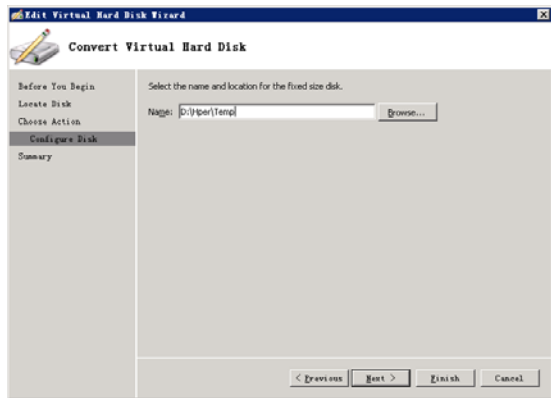


图 24-55 转换虚拟磁盘

⑥ 在“Choose Action”对话框中，选择“Expand”选项，扩展磁盘容量。单击“Next”按钮，显示如图 24-56 所示的“Expand Virtul Hard Disk”对话框。在“New Size”文本框中，键入硬盘的容量。单击“Next”按钮，再单击“Finish”按钮，转换磁盘并关闭该对话框

⑦ 如果选择的硬盘为差异虚拟磁盘，单击“Next”按钮，显示如图 24-57 所示的“Choose Action”对话框，显示磁盘合并功能。

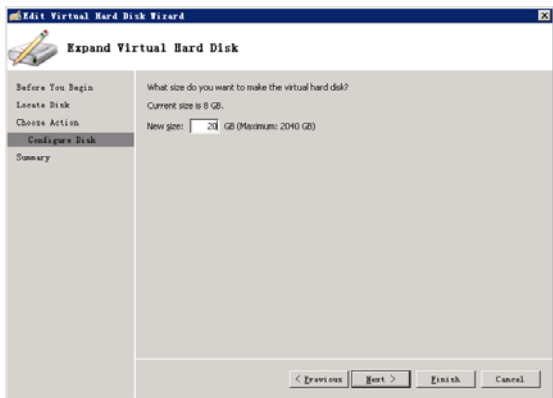


图 24-56 “Expand Virtul Hard Disk”对话

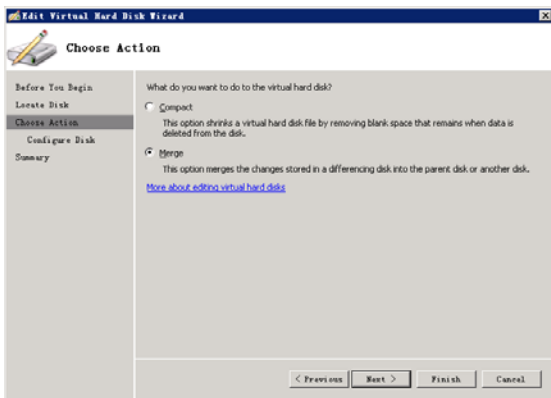


图 24-57 “Choose Action”对话框

⑧ 单击“Next”按钮，显示如图 24-58 所示的“Merge Changes From Differencing Disk”对话框。提供 2 个选项，合并到父虚拟磁盘和合并到新的虚拟磁盘。

⑨ 在“Merge Changes From Differencing Disk”对话框中，选择“To the parent virtual hard disk”选项，将选择的差异虚拟磁盘合并到父虚拟磁盘，单击“Next”按钮，显示如图 24-59 所示的“Completing the Edit Virtual Hard Disk Wizard”对话框。单击“Finish”按钮，完成虚拟磁盘合并。

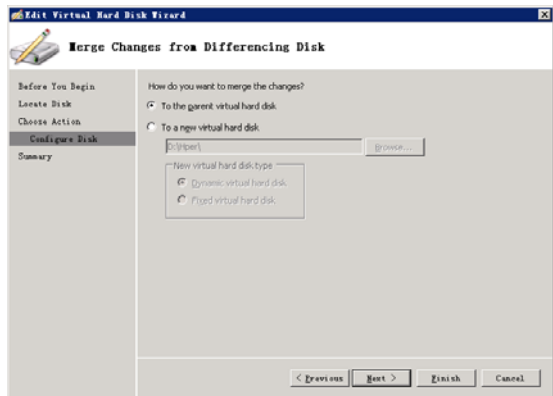


图 24-58 合并虚拟磁盘

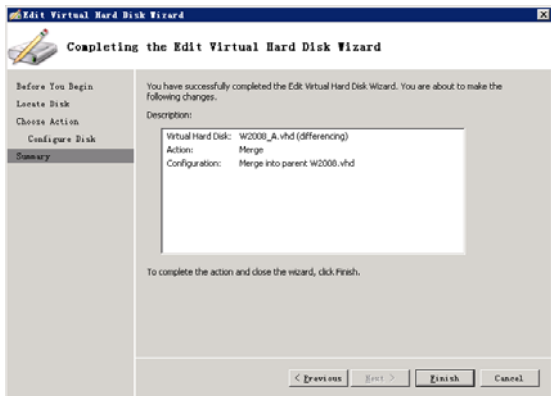


图 24-59 完成磁盘合并

⑩ 在“Merge Changes From Differencing Disk”对话框中，选择“To a new virtual hard disk”选项，将选择的差异虚拟磁盘合并到新虚拟磁盘中。键入新虚拟磁盘的名称，在“New virtual hard disk”对话框中，选择合并后虚拟磁盘的类型。如图 24-60 所示。

⑪ 单击“Next”按钮，显示如图 24-61 所示的“Completing the Edit Virtual Hard Disk Wizard”对话框。单击“Finish”按钮，创建新虚拟磁盘。

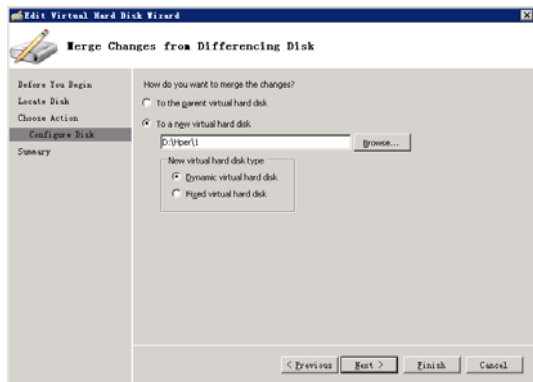


图 24-60 设置虚拟磁盘类型

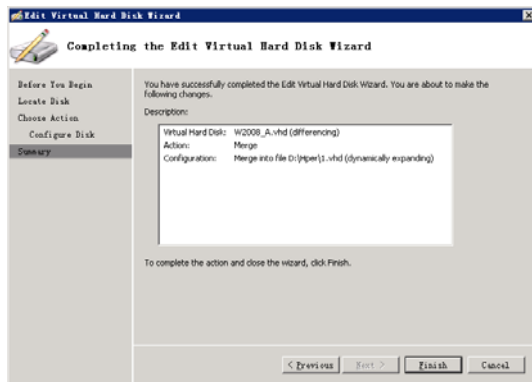


图 24-61 完成虚拟磁盘向导

24.5 创建虚拟机

Hyper-V 和 Virtual PC 2007 以及 Virtual Server 2005 R2 同样采用 VHD 虚拟磁盘格式，三者之间实际上通用，但是并不能直接把 Virtual PC 2007 或者 Virtual Server 2005 R2 的 VHD 磁盘直接挂载到 Hyper-V 虚拟机中。Hyper-V 采用最新的基于 Hypervisor 的 Synthetic 设备硬件架构，在 Hyper-V 虚拟机中，如果子分区中的操作系统发出了一个硬件请求（磁盘请求），对应的 Synthetic 存储设备会知道应该向父分区的物理设备转发请求，子分区和父分区之间会通过高速、点对点的协议 VMBus 进行通信，性能几乎接近物理系统。

24.5.1 创建虚拟机

在 Windows Server 2008 的 Hyper-V 角色中，提供虚拟机创建向导，根据向导即可轻松创建虚拟机。

① 在“服务器管理器”窗口中，单击菜单栏的“操作”菜单，依次选择“New”→“Virtual Machine”，启动创建虚拟机向导。

② 单击“Next”按钮，显示如图 24-62 所示的“Specify Name and Location”对话框。在“Name”文本框中键入虚拟机的名称，默认虚拟机配置文件保存在“C:\ProgramData\Microsoft\Windows\Hyper-V\”目录中。

③ 单击“Next”按钮，显示如图 24-63 所示的“Assign Memory”对话框，设置虚拟机内存。

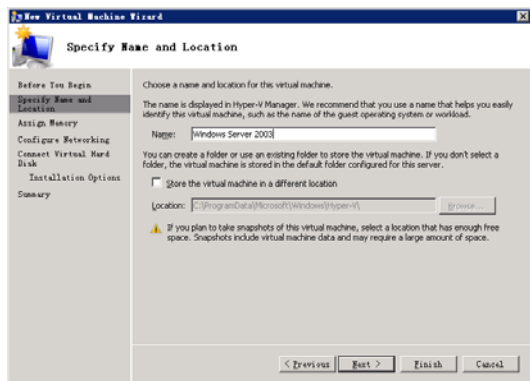


图 24-62 “Specify Name and Location”对话框

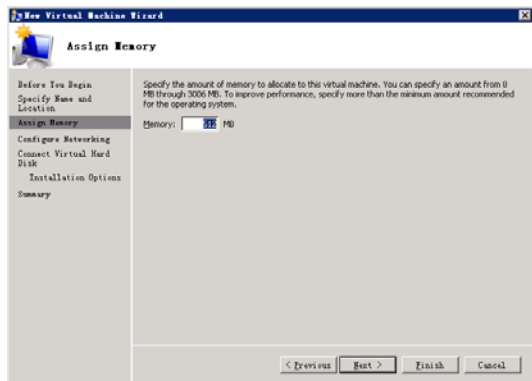


图 24-63 “Assign Memory”对话框

④ 单击“Next”按钮，显示如图 24-64 所示“Configure Networking”对话框，配置虚拟网络，本例中以创建的“内部虚拟机网络”为例说明。

⑤ 单击“Next”按钮，显示如图 24-65 所示“Connect Virtual Hard Disk”对话框，设置虚拟机使用的虚拟磁盘，可以创建一个新的虚拟磁盘，也可以使用已经存在的虚拟磁盘。本例中使用已经创建的虚拟磁盘，选择“Use an existing virtual hard disk”选项，并单击“Browse”按钮，选择虚拟磁盘。

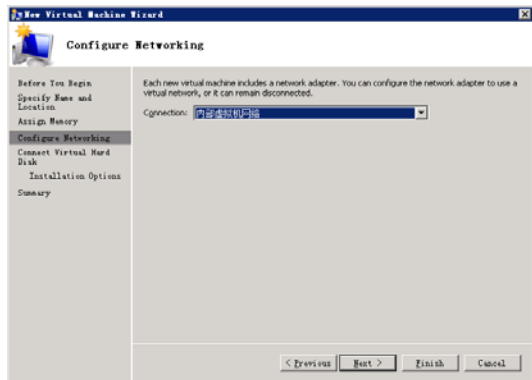


图 24-64 配置网络

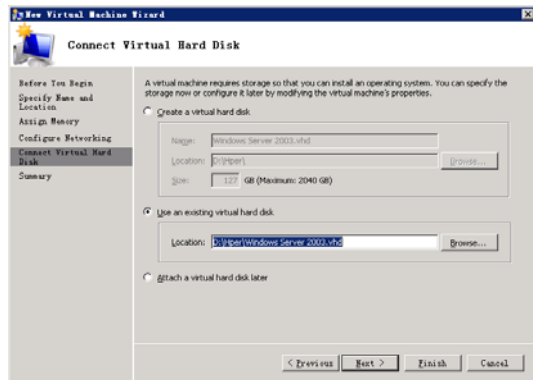


图 24-65 连接虚拟磁盘

⑥ 单击“Next”按钮，显示如图 24-66 所示的“Completing the New Virtual Machine Wizard”对话框，显示虚拟机的配置信息。

⑦ 单击“Finish”按钮，完成虚拟机的创建，如图 24-67 所示。

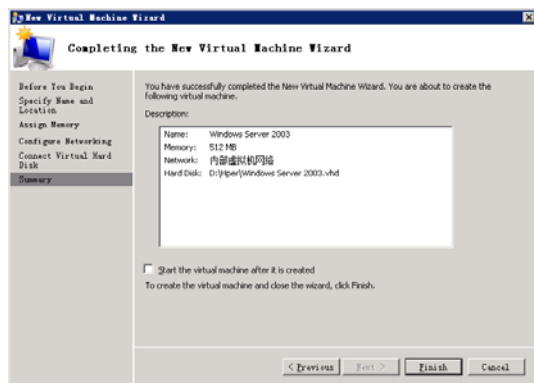


图 24-66 完成配置向导

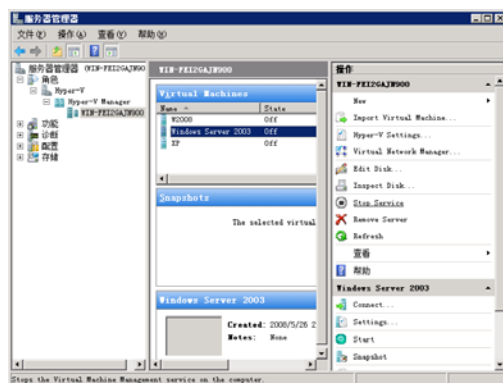


图 24-67 虚拟机创建完成

24.5.2 配置虚拟机属性

虚拟机创建完成后，生成基本虚拟机配置，在虚拟机配置中可以调整其他配置参数，例如内存、硬盘、CD/DVD、SCSI 适配器、网络适配器、软驱、COM 端口与 LPT 端口等。以创建的 Windows Server 2003 虚拟机为例，介绍修改虚拟机配置的方法。

1. Add Hardware 属性

在“服务器管理器”窗口的“Virtual Machines”面板中，选择目标虚拟机，在右侧的“操作”面板中，单击“Settings”超链接，显示“Settings for Windows Server 2003”对话框。虚拟机属性配置分为两大类，分别为：Hardware（硬件）和“Managerment（管理）”。

单击“Hardware”→“Add Hardware”选项，显示如图 24-68 所示。在右侧的允许添加的硬件列表中，显示允许添加的硬件设备，分别为“SCSI 控制器”、“网络适配器”以及“遗留网络适配器”。单击“Add”按钮，可以添加新的硬件。

2. BIOS 属性

单击“Hardware”→“BIOS”选项，显示如图 24-69 所示。在右侧列表中，可以调整硬件设备启动的顺序，默认从“CD”启动。

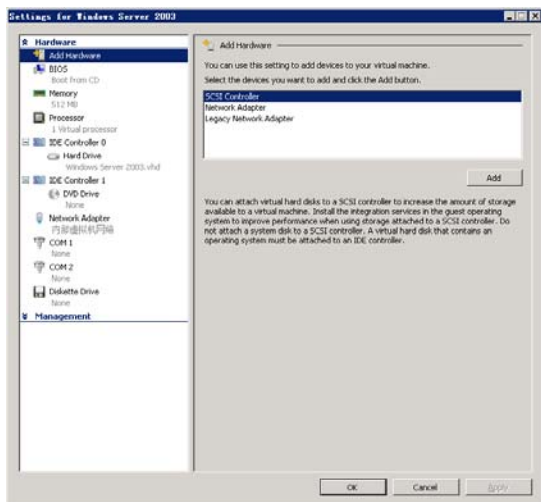


图 24-68 Add Hardware 属性

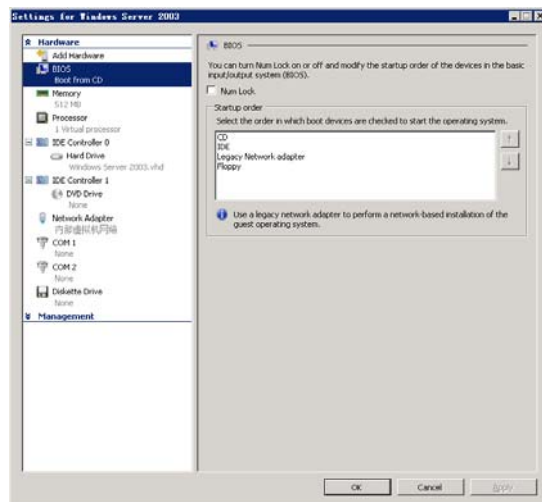


图 24-69 BIOS 属性

3. Memory 属性

单击“Hardware”→“Memory”选项，显示如图 24-70 所示。在“RAM”文本框中，允许修改当前虚拟机的内存。

4. Processor 属性

单击“Hardware”→“Processor”选项，如图 24-71 所示。设置当前虚拟机使用的内核数量，虚拟机使用的内核取决于物理计算机内核的数量，以及虚拟机运行时资源分配状况。

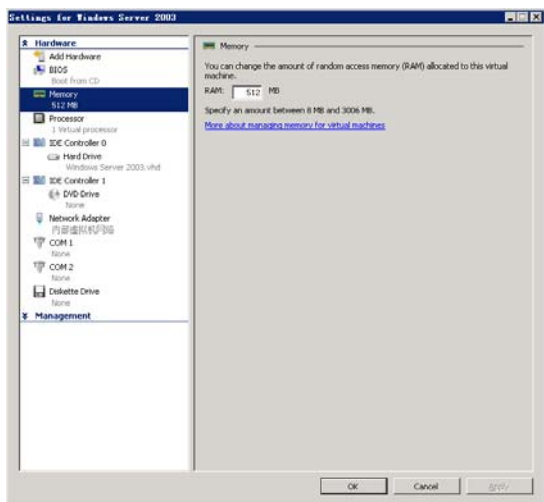


图 24-70 Memory 属性

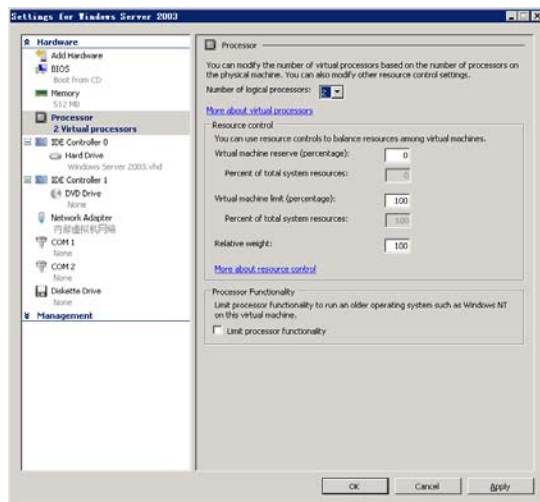


图 24-71 Processor 属性

5. IDE Controller 属性

单击“Hardware”→“IDE Controller 0”选项，显示如图 24-72 所示。在当前 IDE 控制器上，添加新的硬盘或者光盘驱动器。在右侧的列表中选择需要添加的“IDE”控制器，单击“Add”按钮，即可添加新的 IDE 设备，同时允许关联新的虚拟磁盘或者物理光盘驱动器。

6. Network Adapter 属性

单击“Hardware”→“Network Adapter”选项，显示如图 24-73 所示的虚拟机使用的虚拟网络，在右侧的“Network”列表中，可以调整虚拟网络的设置。同时，允许调整该虚拟机的 MAC 地址分配参数，以及所隶属于的 VLAN。

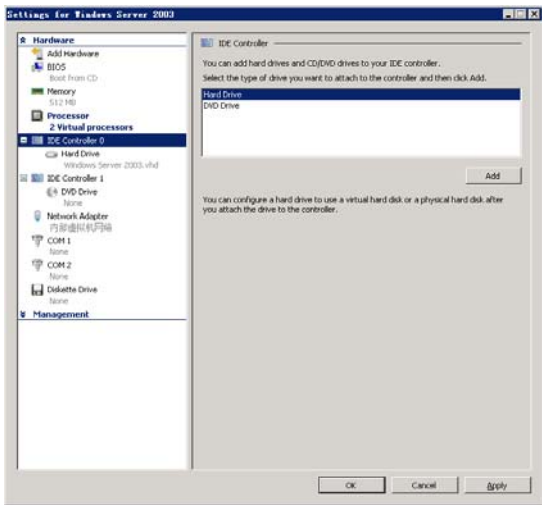


图 24-72 IDE Controller 属性

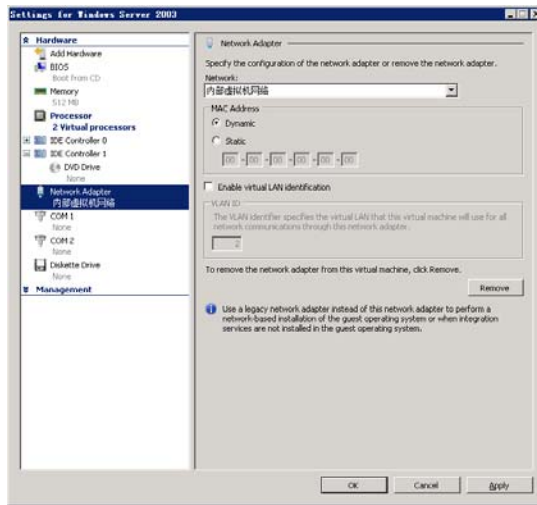


图 24-73 Network Adapter 属性

7. Diskette Drive 属性

单击“Hardware”→“Diskette Drive”选项，显示如图 24-74 所示的对话框，设置虚拟机使用的虚拟软盘驱动器。

8. Name 属性

单击“Management”→“Name”选项，显示如图 24-75 所示的对话框，编辑当前虚拟机的名称以及描述信息。

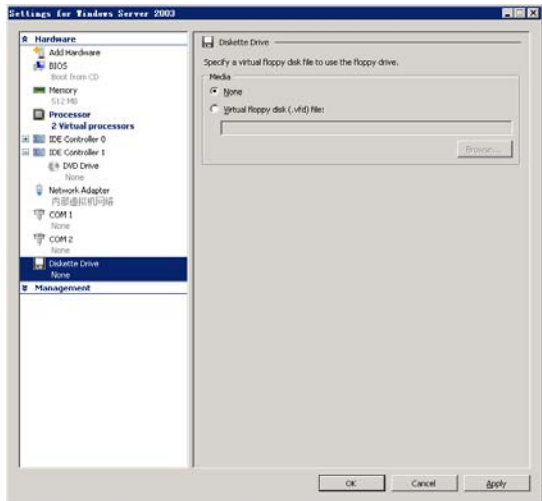


图 24-74 Diskette Drive 属性

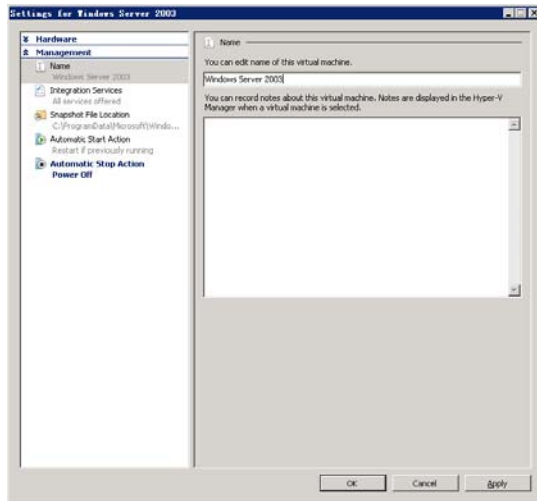


图 24-75 Name 属性

9. Snapshot File Location 属性

单击“Management”→“Snapshot File Location”选项，显示如图 24-76 所示的对话框，设置虚拟机快照存储位置，默认存储在“C:\ProgramData\Microsoft\Windows\Hyper-V”目录中。

10. Automatic Start Action 属性

单击“Management”→“Automatic Start Action”选项，显示如图 24-77 所示，设置虚拟机当物理计算机启动时虚拟机执行的操作，建议选择“None”选项，以加快物理计算机的执行效率。

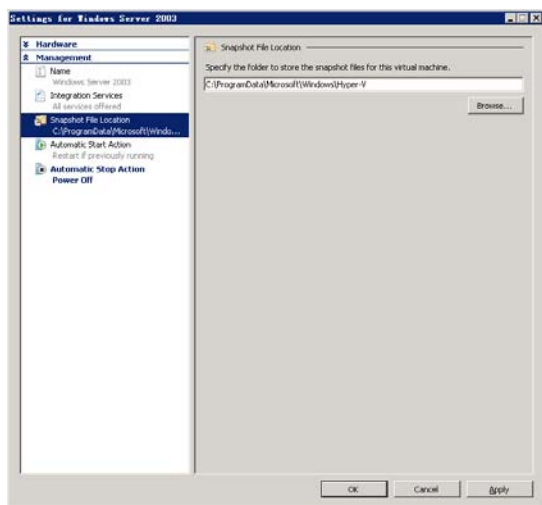


图 24-76 Snapshot File Location 属性

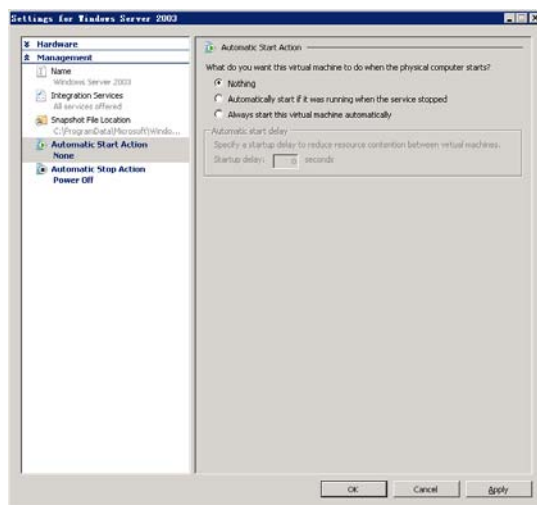


图 24-77 Automatic Start Action 属性

11. Automatic Stop Action 属性

单击“Management”→“Automatic Stop Action”选项，显示如图 24-78 所示，设置虚拟机当物理计算机关闭时虚拟机执行的操作，建议选择“Turn Off the virtual machine”选项，关闭物理计算机时，同时关闭虚拟机。

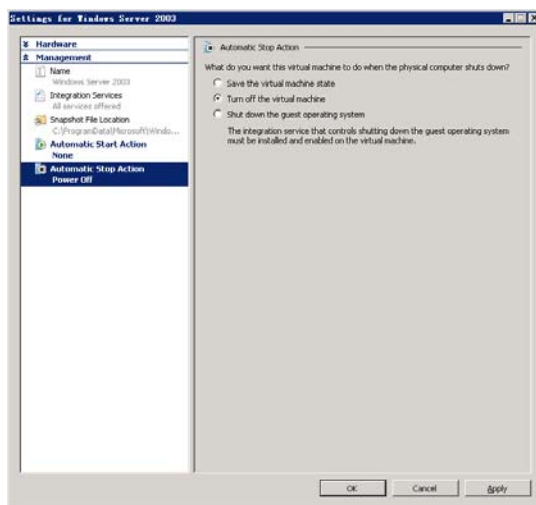


图 24-78 Automatic Stop Action 属性

24.5.3 安装虚拟机操作系统

以 Windows Server 2003 操作系统为例，说明在 Windows Server Virtualization 环境中安装操作系统的方法。

① 在“服务器管理器”窗口的“Virtual Machines”面板中，选择目标虚拟机“Windows Server 2003”，在右侧的“操作”面板中单击“Settings”超链接，启动“Settings for Windows Server 2003”对话框，如图 24-79 所示。

② 选择“Hardware”→“IDE Controller 1”选项，如图 24-80 所示，在“Media”分组框中，选

择“Image File”选项。单击“Browse”按钮，选择 Windows Server 2003 操作系统映像光盘。

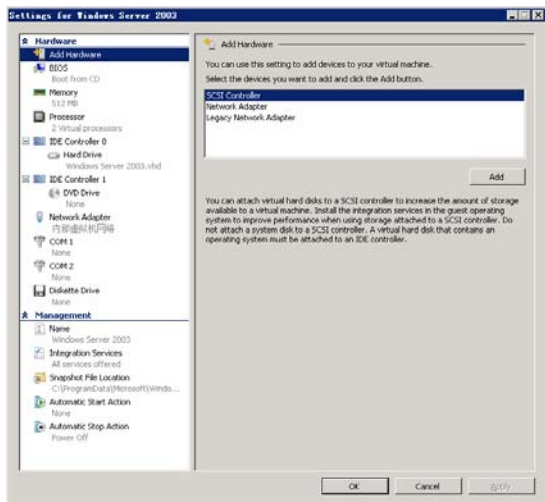


图 24-79 设置 Windows Server 2003

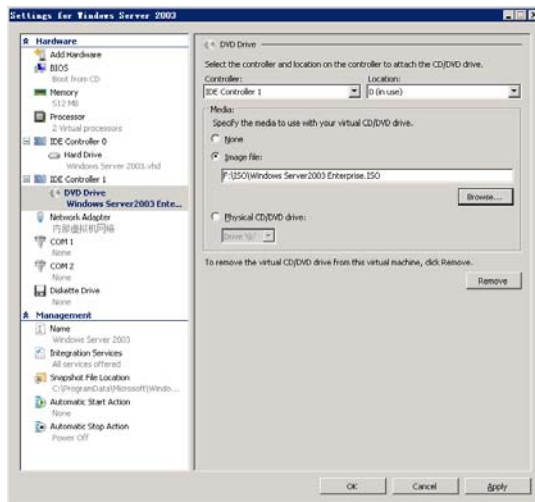


图 24-80 选择映像光盘

③ 单击“OK”按钮，关闭“Settings for Windows Server 2003”对话框，返回到“服务器管理器”窗口中。

④ 在“服务器管理器”窗口右侧的“操作”面板中，单击“Start”超链接，如图 24-81 所示，以光盘启动模式引导虚拟机。

⑤ 在“服务器管理器”窗口的“Virtual Machines”面板中，右击目标虚拟机“Windows Server 2003”，在快捷菜单中选择“Connect”命令，即可启动 Windows Server 2003 并进行安装。如图 24-82 所示。

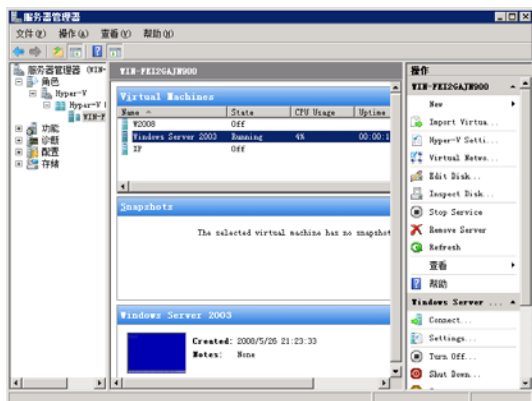


图 24-81 启动虚拟机

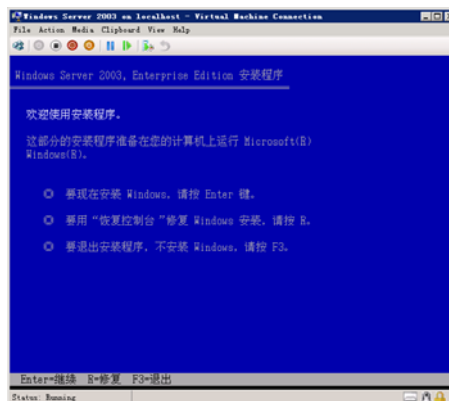


图 24-82 安装 Windows Server 2003



《网络服务搭建、配置与管理大全 (Windows 版)》

读者交流区

尊敬的读者：

感谢您选择我们出版的图书，您的支持与信任是我们持续上升的动力。为了使您能通过本书更透彻地了解相关领域，更深入的学习相关技术，我们将特别为您提供一系列后续的服务，包括：

1. 提供本书的修订和升级内容、相关配套资料；
2. 本书作者的见面会信息或网络视频的沟通活动；
3. 相关领域的培训优惠等。

请您抽出宝贵的时间将您的个人信息和需求反馈给我们，以便我们及时与您取得联系。

您可以任意选择以下三种方式与我们联系，我们都将记录和保存您的信息，并给您提供不定期的信息反馈。

1. 短信

您只需编写如下短信：B07880+您的需求+您的建议

发送到1066 6666 789（本服务免费，短信资费按照相应电信运营商正常标准收取，无其他信息收费）

为保证我们对您的服务质量，如果您在发送短信24小时后，尚未收到我们的回复信息，请直接拨打电话（010）88254369。

2. 电子邮件

您可以发邮件至jsj@phei.com.cn**或**editor@broadview.com.cn**。**

3. 信件

您可以写信至如下地址：北京万寿路173信箱博文视点，邮编：100036。

如果您选择第2种或第3种方式，您还可以告诉我们更多有关您个人的情况，及您对本书的意见、评论等，内容可以包括：

- （1）您的姓名、职业、您关注的领域、您的电话、E-mail地址或通信地址；
- （2）您了解新书信息的途径、影响您购买图书的因素；
- （3）您对本书的意见、您读过的同领域的图书、您还希望增加的图书、您希望参加的培训等。

如果您在后期想退出读者俱乐部，停止接收后续资讯，只需发送“B07880+退订”至10666666789即可，或者编写邮件“B07880+退订+手机号码+需退订的邮箱地址”发送至邮箱：market@broadview.com.cn 亦可取消该项服务。

同时，我们非常欢迎您为本书撰写书评，将您的切身感受变成文字与广大书友共享。我们将挑选特别优秀的作品转载在我们的网站（www.broadview.com.cn）上，或推荐至CSDN.NET等专业网站上发表，被发表的书评的作者将获得价值50元的博文视点图书奖励。

我们期待您的消息！

博文视点愿与所有爱书的人一起，共同学习，共同进步！

通信地址：北京万寿路 173 信箱 博文视点（100036）

E-mail：jsj@phei.com.cn，editor@broadview.com.cn

电话：010-51260888

www.phei.com.cn

www.broadview.com.cn

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：（010）88254396；（010）88258888

传 真：（010）88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036